Algebra

Course by: Professor Richard Borcherds
Notes by: Jackson Van Dyke[0.1]

Fall 2017

[0.1] Any errors introduced are my own.

Contents

0.1 Introduction . . . 5

1 Groups 6

1.1 Definitions . . . 6

1.2 Lagrange's theorem and product groups . . . 8

1.2.1 Groups of order 1, 2, 3 . . . 8

1.2.2 Groups of order 4, 5 . . . 10

1.2.3 Products . . . 11

1.3 Quotient groups . . . 12

1.3.1 Normal subgroups . . . 12

1.3.2 Groups of order 6 . . . 13

1.3.3 Exact sequences . . . 16

1.4 Groups of order 8 . . . 17

1.4.1 Dihedral Group . . . 18

1.4.2 Quaternions . . . 19

1.5 Groups of order p^2 . . . 21

1.6 Nilpotent groups . . . 23

1.7 Groups of order $2p$ . . . 23

1.8 Groups of order 12 . . . 24

1.8.1 Dihedral, binary dihedral groups . . . 24

1.8.2 Rotations of tetrahedron . . . 24

1.8.3 Sylow theorems . . . 25

1.8.4 Solvability . . . 26

1.9 Groups of order $13 - 16$ . . . 28

1.9.1 Groups of order pq . . . 28

1.9.2 Groups of order 16 . . . 28

1.10 Finitely Generated Abelian Groups . . . 29

1.11 Groups of order $17 - 24$ . . . 30

1.12 Symmetric Group . . . 31

1.12.1 Definitions, examples . . . 31

1.12.2 Alternating group . . . 31

1.12.3 Platonic Solids . . . 32

1.12.4 Conjugacy Classes . . . 32

1.12.5 Normal subgroups of S_n . . . 33

1.12.6 Automorphisms . . . 34

1.13 Category Theory . . . 35
1.13.1 Definitions . . . 35
1.13.2 Functors . . . 36
1.13.3 Natural Transformations . . . 38
1.13.4 Products, equalizers . . . 38
1.13.5 Universality . . . 39
1.13.6 Limits, Colimits . . . 40
1.14 Free groups . . . 42
1.14.1 Free abelian groups . . . 42
1.14.2 Free groups . . . 43
1.14.3 Subgroups of free groups . . . 45

2 Rings 48
2.1 Definitions and examples . . . 48
2.2 Group rings . . . 50
2.3 Ideals . . . 51
2.4 Generators and relations . . . 52
2.5 Integral domains . . . 52
2.5.1 Euclidean domains . . . 53
2.5.2 Principle Ideal Domains . . . 53
2.5.3 Unique factorization domains . . . 54
2.6 Ideals of commutative rings . . . 57
2.6.1 Zorn's Lemma . . . 58
2.7 Localization . . . 60
2.7.1 Motivation and Construction . . . 60
2.7.2 Examples . . . 62

3 Modules 64
3.1 Definitions . . . 64
3.2 Examples . . . 65
3.3 Free modules . . . 66
3.4 Projective modules . . . 67
3.5 Tensor products . . . 71
3.5.1 Construction . . . 71
3.5.2 Exact sequences . . . 72
3.5.3 Noncommutative rings . . . 76
3.6 Duality . . . 76
3.6.1 Definition and examples . . . 76
3.6.2 Dirichlet characters . . . 77
3.6.3 Fourier transforms . . . 78
3.6.4 Injective modules . . . 79
3.7 Limits, colimits . . . 80
3.7.1 Definitions, examples . . . 80
3.7.2 Exact sequences and direct limits . . . 81
3.7.3 Inverse limits, p-adic integers . . . 83
3.8 Snake Lemma . . . 84

3.8.1 Statement and proof of the lemma 84
3.8.2 Tor 86
3.8.3 Mittag-Leffler condition 88
3.9 Finitely generated modules over a PID 90

4 Polynomials 91
4.1 Preliminaries 91
4.2 Application to fields 93
4.3 Unique factorization in polynomial rings 93
4.4 Irreducibility 95
4.4.1 Basic algorithms 95
4.4.2 Eisenstein's Criterion 96
4.4.3 Rational roots 97
4.5 Noetherian rings and polynomials 98
4.5.1 Noether's theorem 98
4.5.2 Hilbert's Theorem 99
4.6 Invariants and symmetric functions 100
4.6.1 The discriminant 102
4.6.2 Conditions for common factors 103
4.6.3 Ring of invariants 104
4.7 Formal power series 106
4.7.1 Definitions 106
4.7.2 Ideals and condition for being Noetherian 107
4.7.3 Weierstrass preparation theorem 108
4.7.4 Hensel's Lemma 110

5 Algebraic extensions 112
5.1 Field extensions 112
5.2 Splitting fields 115
5.2.1 Finite fields 116
5.3 Algebraic closure 117
5.4 Normal extensions 118
5.5 Separable extensions 119
5.6 Galois extensions 120
5.7 Main theorem of Galois theory 121
5.8 Intermediate field extensions 122
5.9 Normal extensions and normal subgroups 125
5.10 Applications to polynomials 128
5.10.1 Algebraic closure of $\mathbb{C}$ 128
5.10.2 Structure of separable extensions 129
5.11 Cyclic extensions 130
5.11.1 Prime order 130
5.11.2 Solvable Galois groups 132
5.12 Cyclotomic polynomials 133
5.12.1 Examples and definitions 133
5.12.2 Prime numbers 135

5.12.3 Rational Galois extensions 135
5.12.4 Finite division algebras 136
5.13 Norm and trace 137
5.13.1 Definitions and basic properties 137
5.13.2 Algebraic integers 138
5.13.3 Trace as a bilinear form 140
5.13.4 Discriminants of field extensions 141
5.13.5 Properties of the norm 144
5.13.6 Hilbert's theorem 90 145
5.14 Solving equations 146
5.14.1 Cubic equation 146
5.14.2 Quartic equation 148
5.15 Galois cohomology 149
5.15.1 Definitions and examples 149
5.15.2 Alternative definition 151
5.15.3 General form of Hilbert's theorem 90 151
5.16 Infinite Galois extensions 154
5.16.1 Profinite groups and Krull topology 154
5.16.2 Galois correspondence 156
5.17 Kummer theory 158

0.1 Introduction

These notes were taken during the course math 250A in fall 2017 at UC Berkeley. The professor was Richard Borcherds, to whom I defer credit for all of the mathematical content in this document. I myself claim ownership of all the errors in this document, of which there are likely many.

This course is meant to serve as an early graduate algebra course. Roughly speaking, the first part concerns itself over groups, the second moves to rings, modules, and polynomials, and the final portion focuses on field extensions and Galois theory. Though I made an effort to keep these notes logically self-contained, there will likely be some portions that assume some previous knowledge of algebra.

If you have any questions, suggestions, or comments concerning these notes, please do not hesitate to contact me at jacksontvandyke@gmail.com.

Chapter 1

Groups

1.1 Definitions

Definition 1.1 (Concrete group)**.** A set G is a group iff it is the set of symmetries of something.

Example 1.1. We can consider the symmetries of a rectangle to be: doing nothing, reflecting (horizontal and vertical), and rotating. We will be returning to this geometric interpretation later.

Definition 1.2 (Abstract group)**.** A set G with a binary relation (if $a, b \in G$, written $a \times b, a + b, a \cdot b, a \circ b$ or just ab) is a group iff this relation is associative, each element has an inverse, and there is an identity. In other words, for all $a, b, c \in G$,

1. There exists $e \in G$ such that $ea = ae = a$
2. There exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$
3. $a\left(bc\right) = \left(ab\right)c$

Remark 1.1. It is clear that if we take the composition of symmetries as our binary relation, then the concrete notion of a group can be translated to the abstract notion. It is a subtle and important point that the converse is true. First we consider some basic definitions.

Definition 1.3 (Subgroup)**.** Let G be a group. A subset $H \subseteq G$ is a *subgroup* of G iff it contains the identity of G, is closed under the law of composition, and contains all inverses.

Definition 1.4 (Homomorphism)**.** Let G, H be two groups. Then a function $f : G \to H$ is a homomorphism iff for all $a, b \in G$,

$$f\left(ab\right) = f\left(a\right) f\left(b\right) \tag{1.1}$$

Proposition 1.1. *Homomorphisms preserve inverses and the identity.*

Proof. Let G, H be groups, and take $f : G \to H$ to be a homomorphism. Then for all $g \in G$ we have that

$$f(g) = f(ge) = f(g) f(e) = f(eg) = f(e) f(g) \tag{1.2}$$

then by the definition, and uniqueness of the identity element, $f(e)$ is the identity in H. Then if we have $a \in G$ with inverse a^{-1} we can write

$$f(e) = f\left(aa^{-1}\right) = f(a) f\left(a^{-1}\right) = f\left(a^{-1}a\right) = f\left(a^{-1}\right) f(a) \tag{1.3}$$

so since f preserves the identity, we have that it also preserves inverses. □

Definition 1.5 (Isomorphism)**.** A homomorphism is an *isomorphism* iff it is a bijection.

Definition 1.6 (Endomorphism)**.** A homomorphism is an *endomorphism* iff it has the same domain as its codomain.

Definition 1.7 (Automorphism)**.** A homomorphism is an *automorphism* iff it is an isomorphism and an endomorphism.

Example 1.2. Let $G = \langle \mathbb{R}, + \rangle$ and $H = \langle \mathbb{R}^{\times}, \times \rangle$. Then if we take $f : G \to H$ to be the exponential map, we get an isomorphism.

Definition 1.8. Let G be a group and S a set. Then a map $\cdot : G \times S \to S$ is a *left action* of G on S iff for all $s \in S$ and all $g, h \in G$ we have:

1. $g \cdot (h \cdot s) = (gh) \cdot s$
2. $e \cdot s = s$

where e is the identity for G. A *right action* is a map $\cdot : S \times G \to S$ which satisfies the analogous properties.

Definition 1.9. Let G be a group. A set S is a G-set iff we have an action of G on S which is a homomorphism

$$\pi : G \to \mathrm{Perm}(S) \tag{1.4}$$

Example 1.3. Let G be a group, and S a G-set. Then the image of G in $\mathrm{Perm}(S)$ is a subgroup of $\mathrm{Perm}(S)$.

Theorem 1.1. *A set G is an abstract group iff it is a concrete group.*

Proof. $(\Longleftarrow)$: Suppose G is a concrete group. Then take composition of symmetries as the binary relation, and we see that this structure satisfies the axioms of an abstract group.

$(\implies)$: Suppose G is an abstract group. We desire to find some object S such that G comprises the symmetries of S which preserve whatever structure is on S. Explicitly we take S to be a G-set, and consider the right action of

G on S to be such a structure. A symmetry $f : S \to S$ is said to preserve the right action $\cdot : S \times G \to S$ iff for all $g \in G$ and all $s \in S$, $f(s \cdot g) = f(s) \cdot g$. In other words the symmetry commutes with the right action. Now notice that if we set $S = G$ we get such a symmetry automatically from the left action of G on itself. This preservation follows directly from the associativity given in the definition of an abstract group. This means we have shown that the left action of a group G on itself, is a symmetry of G which respects the structure given by the right action of G on itself.

We now wish to show, that every symmetry $f : S \to S$ which commutes with the right action of G on S is given by the left action of some element $g \in G$. We know $f(e) = g$ for some g since we set $S = G$ and we can write that

$$f(s) = f(es) = f(e) \cdot s = g \cdot s \tag{1.5}$$

So f is effectively the "same" as g, and therefore every such symmetry f is given by some $g \in G$. □

We can picture G as a graph, where the elements are vertices, and the edges between elements are labeled by their right actions. Then the left action of G gives the symmetries of the graph.

Lemma 1.1. *If we have a left action of a group G on a set S, then we automatically have a right action and vice versa. In particular, we write*

$$s \cdot g = g^{-1} s \tag{1.6}$$

to define a right action in terms of a given left action.

Proof. To see this, we write:

$$s(gh) = (gh)^{-1} s = h^{-1}\left(g^{-1} s\right) = (sg)h \tag{1.7}$$

as desired. □

Proposition 1.2. *There are 8 types of actions of a group on itself. There are four right, and four left actions on a group. We only list the left four.*

1. *Trivial:* $g \cdot s = s$
2. *Left:* $g \cdot s = gs$
3. *Right (to Left):* $g \cdot s = sg^{-1}$
4. *Adjoint (Conjugation)*[1.1] *:* $g \cdot s = gsg^{-1}$

1.2 Lagrange's theorem and product groups

1.2.1 Groups of order 1, 2, 3

Proposition 1.3. *The only group of order 1 is the trivial group.*

Definition 1.10 (Coset)**.** Let G be a group and $H \subseteq G$ a subgroup. Then the *left cosets* of H are sets of the form $gH = \{gh \,|\, h \in H\}$ for any $g \in G$. The *right cosets* of H are sets of the form $Hg = \{hg \,|\, h \in H\}$ for any $g \in G$.

Theorem 1.2 (Lagrange)**.** *Let G be a group, and $H \subseteq G$ be a subgroup. If both $|H|, |G|$ are finite, then $|H|$ divides $|G|$.*

Proof. To prove this we look at the cosets of H. We notice that all cosets have the same order, and any two are either equal or disjoint. In particular, if $g_1 h_1 = g_2 h_2$ then for any h we have that $g_1 h = g_2 h_2 h_1^{-1} h \in g_2 H$ as desired. The map $h \mapsto gh$ is a bijection from H into gH, with obvious inverse. Therefore,

$$|G| = \text{ number of left cosets of } H \times |H| \tag{1.8}$$

and we are done. □

Corollary 1.1. *There is only one group of prime order.*

Proof. Let G be a group such that $|G| = p < \infty$ for prime p. Consider any $g \in G$. We know $|g| = |\langle g \rangle|$ also has order dividing $|G|$ from Lagrange's theorem. If $|g| = 1$, then $g = e$. Otherwise the order of g is p and therefore all other elements of G are $1, g, \cdots, g^{p-1}$ where $p^a p^b = p^{ab \,(\text{mod}\, p)}$. In particular, G is cyclic. □

Applications

Theorem 1.3 (Fermat's little theorem)**.** *Let $a, p \in \mathbb{Z}$ and p prime, then*

$$a^{p-1} = 1 \pmod{p} \tag{1.9}$$

Proof. If $a = 0$, this is trivial, so we take $a \neq 0$. Look at $(\mathbb{Z}/p\mathbb{Z})^\times$ under multiplication. We can also take $\tilde{a} \coloneqq a \bmod p \in (\mathbb{Z}/p\mathbb{Z})^\times$ by definition. Since this is a group of order $p-1$ every element has order dividing $p-1$. Formally, there exists $n \in \mathbb{Z}$ such that $|\tilde{a}|\, n = p - 1$. This means, we can write

$$\tilde{a}^{p-1} = \tilde{a}^{|\tilde{a}| n} = e \tag{1.10}$$

as desired. □

Definition 1.11. A function $\varphi : \mathbb{Z} \to \mathbb{N}$ is called the *Euler totient function* iff it returns the number of integers between the argument and zero, which are relatively prime to the argument.

Example 1.4. Let φ be the Euler totient function. Then we have $\varphi(5) = 4$ and $\varphi(6) = 2$ to name a few easy examples. For prime p, $\varphi(p) = p - 1$ and $\varphi(p^n) = p^n - p^{n-1} = p^n (1 - 1/p)$ for $n \in \mathbb{Z}^+$. If $p, q \in \mathbb{Z}$ are relatively prime, then $\varphi(pq) = \varphi(p)\varphi(q)$.

Proposition 1.4. *If φ is Euler's totient function and $n \in \mathbb{Z}$, then*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{1.11}$$

where the product is over all distinct prime integers p dividing n.

Theorem 1.4 (Euler's little theorem)**.** *Take integers $g, m \in \mathbb{Z}$ such that $(g, m) = 1$. It is then the case that*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{1.12}$$

where φ is the Euler's totient function.

Proof. Let $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$ under multiplication. Then $|G| = \varphi(n)$. Now by Lagrange's theorem, for all $g \in G$ we have $g^{\varphi(n)} = e$. as desired. □

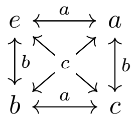
Example 1.5. It is helpful to consider a geometric notion of Lagrange's theorem. Suppose G acts on a set S transitively for some g. This means for any $s, t \in S$ there is some $g \in G$ such that we get $s = g \cdot t$.

Now take $H = \{h \in G \,|\, \forall s \in S,\, h \cdot s = s\}$ then we have a correspondence between points of S and cosets of H by sending $t \in S$ to $\{g \in G \,|\, g \cdot s = t\}$ which is a coset of H, since if $g \cdot s = t$ then for $h \in H$, $(gh) \cdot s = t$ since $h \cdot s = s$. In the other direction we send any coset gH to the point $g \cdot s$.

Example 1.6. Explicitly, if we have some geometric solid, we can find the order of the corresponding group to be the number of fixings of a face, multiplied by the number of faces. For an icosahedron, the number of symmetries comes out to be $3 \times 20 = 60$.

1.2.2 Groups of order 4, 5

Example 1.7. There are two examples of this order. In particular, these are: $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ and the symmetries of a rectangle.



+	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Now the orders of the elements can be used to determine these groups are not isomorphic:

Element:	0	1	2	3
Order:	1	4	2	4

Element:	1	a	b	c
Order:	1	2	2	2

Lemma 1.2. *If all elements have order 2 the group is abelian.*

Proof. Let G be a group. Take $g, h \in G$. We have $1 = (gh)^2 = ghgh$ and $1 = g^2h^2 = gghh$ so $gh = hg$. □

Proposition 1.5. *There are only two groups of order 4. In particular, they are the ones above.*

Proof. Let G be a group of order 4. Lagrange's theorem implies that all elements of G have order $1, 2$ or 4. If some element has order 4, then all of the elements are $1, g, g^2, g^3$ where $g^a g^b = g^{a+b \,(\mathrm{mod}\, 4)}$ so we have the cyclic case as above and the group is isomorphic to $\langle \mathbb{Z}/4\mathbb{Z}, +\rangle$.

Then if we have all elements of order 2, by the preceding lemma, we have that G is abelian. Now writing additively, G is a vector space over the field $\mathbb{F}_2$. This means G is isomorphic to the unique 2 dimensional vector space over F_2. This implies there are only two groups of order 4. □

Proposition 1.6. *The group of order* 5 *is unique up to isomorphism.*

Proof. Since 5 is prime, we have this directly from corollary 1.1. □

1.2.3 Products

Definition 1.12 (Product)**.** Let G, H be groups. The group $G \times H$ is the *product* of G and H iff it is the cartesian product of G and H equipped with a binary relation given by the component operations of G and H. Explicitly:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \tag{1.13}$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$.

Example 1.8. We list some examples of product groups:

- $\{1, a, b, c\} \cong \{1, a\} \times \{1, b\}$ where explicitly we map $1 \mapsto (1, 1), a \mapsto (a, 1), b \mapsto (1, b), c \mapsto (a, b)$.
- $\langle \mathbb{Z}^\times, \times\rangle \cong \{-1, 1\} \times \mathbb{Z}^+$
- $\langle \mathbb{R}^\times, \times\rangle \cong \{-1, 1\} \times \mathbb{R}^+$
- $\mathbb{C}^\times \cong S^1 \times \mathbb{R}^+$
- For F a finite field, the vector space F_n is the product of n copies of F under addition.

Example 1.9. Consider the group G of all the roots of unity in $\mathbb{C}$. First note that G is isomorphic to $\mathbb{Q}/\mathbb{Z}$. This is given by $\frac{m}{n} \mapsto \exp(2\pi i m/n)$ Then we have that

$$G := \{z \in \mathbb{C} \mid z = \exp 2\pi m/n,\ m, n \in \mathbb{Z}\} \tag{1.14}$$

so if we define:

$$H_1 = \left\{z \in G \mid \exists n \in \mathbb{Z}, z^{2n+1} = 1\right\} \tag{1.15}$$

$$H_2 = \left\{z \in G \mid \exists n \in \mathbb{Z}, z^{2n} = 1\right\} \tag{1.16}$$

then we have that $G = H_1 \times H_2$. In fact we could have done this for any prime not just 2.

Proposition 1.7. *To see if* $G = H_1 \times H_2$ *we have to check*

1. *Anything in G is of form $h_1 \times h_2$ for $h_1 \in H_1, h_2 \in H_2$*
2. *$H_1 \cap H_2 = e$*
3. *H_1 commutes with H_2*

1.3 Quotient groups

1.3.1 Normal subgroups

Example 1.10. Let G be a group, and $H \subseteq G$ a subgroup. Then define

$$G/H \coloneqq \{aH : a \in G\} \tag{1.17}$$

Is G/H a group? Consider two cosets aH, bH. Define the product in the natural way. When is this well defined? We formally define an equivalence relation:

$$a \equiv b \iff aH = bH \left(ab^{-1} \in H\right) \tag{1.18}$$

Then we wonder if $a_1 \equiv a_2$, and $b_1 \equiv b_2$ is $a_1b_1 \equiv a_2b_2$? Only sometimes. Suppose $b_1 \equiv b_2$, then there exists $h \in H$ such that $b_1 = b_2h$. Then $ab_1 = ab_2h$ so

$$ab_1 \equiv ab_2 \tag{1.19}$$

Now suppose $a_1 \equiv a_2$ so there is some $h \in H$ such that $a_1 = a_2h$. Then we want:

$$a_1b = a_2hb \equiv a_2b \tag{1.20}$$

So we want these to generate the same left coset. In other words, we need to "move" h past b. This is clearly allowed if the group is commutative. More generally, we can insist that there exists some $h' \in H$ such that $hb = bh'$, or equivalently that $b^{-1}Hb = H$. Then we have that G/H forms a group since the natural multiplication of cosets is well defined. This is a kind of subgroup which commutes with the group.

Definition 1.13. Let G be a group, and H a subgroup. Then H is *normal* iff for all $g \in G$, $gH = Hg$.

Remark 1.2. A subgroup H is normal iff the left cosets are the same as the right cosets.

Proposition 1.8. *The cosets of a normal subgroup form a group under the multiplication of representative elements.*

Proof. This is identical to the discussion in example 1.10. □

Definition 1.14. Let $N \subseteq G$ be a normal subgroup. Then G/N is the *quotient group* of G by N.

Example 1.11. If we have $G = S_3$, then the subgroup $H = \{e, \left(1\,2\,3\right) \left(1\,3\,2\right)\}$ is normal. Recall that the notation $\left(a\,b\,c\,d\right)$ means a function mapping

$$a \mapsto b \mapsto c \mapsto d \mapsto a \tag{1.21}$$

Theorem 1.5. *Any subgroup of index* 2 *is normal.*

Proof. If H has index 2 then the left cosets are just H, and the things not in H. Then these are also the right cosets, so G/H is a group of order 2. □

Example 1.12. Let $G = S_3$ then $G \supseteq H = \{e, \left(1\,2\right)\}$ is not normal. To see this, notice that $\left(2\,3\right)\left(1\,2\right)\left(2\,3\right)^{-1} = \left(1\,3\right)$ so $\left(2\,3\right) H \left(2\,3\right)^{-1} \neq H$. In particular, since $\left(2\,3\right)\left(1\,2\right) = \left(1\,3\,2\right)$ and $\left(3\,1\right)\left(1\,2\right) = \left(1\,2\,3\right)$ we have that the left and right cosets of H are:

- Left: $\{e, \left(1\,2\right)\}, \{\left(2\,3\right), \left(1\,3\,2\right)\}, \{\left(3\,1\right), \left(1\,2\,3\right)\}$
- Right: $\{e, \left(1\,2\right)\}, \{\left(2\,3\right), \left(1\,2\,3\right)\}, \{\left(3\,1\right), \left(1\,3\,2\right)\}$

1.3.2 Groups of order 6

Proposition 1.9. *There is* 1 *abelian, cyclic group of order* 6*. It also splits as the following product*[1.2]

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \tag{1.22}$$

The lattice of subgroups is given as:

$$\begin{tikzcd}
 & \mathbb{Z}/6\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
A = \{0,2,4\} \arrow[dr, dash] & & B = \{0,3\} \arrow[dl, dash] \\
 & \{0\} &
\end{tikzcd}$$

Proposition 1.10. *Let $G = \mathbb{Z}/6\mathbb{Z}$ and A, B be as in the above diagram. We have that $G \cong A \times B$.*

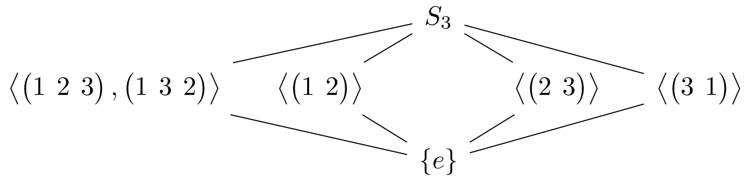
Proof. We check that $G = AB$, $A \cap B = \{0\}$, and $AB = BA$, and the result follows directly from this. □

Proposition 1.11. *The other group of order* 6 *is the symmetric group S_3 given by*

Element:	e	$\left(1\,2\right)$	$\left(2\,3\right)$	$\left(3\,1\right)$	$\left(1\,2\,3\right)$	$\left(1\,3\,2\right)$
Order:	1	2	2	2	3	3

The subgroups are:

[1.2] Cayley made the famous mistake of once saying that there are three groups of order 6, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and S_3.


S_3
$\left\langle \left(1\ 2\ 3\right), \left(1\ 3\ 2\right) \right\rangle$
$\left\langle \left(1\ 2\right) \right\rangle$
$\left\langle \left(2\ 3\right) \right\rangle$
$\left\langle \left(3\ 1\right) \right\rangle$
$\{e\}$

Remark 1.3. $R = \left\{e, \left(1\,2\,3\right), \left(1\,3\,2\right)\right\}$ is the subgroup of rotations.

We now consider whether these are all of the groups of order 6…We want to pick an element of order 3, but how do we know this element exists?

Definition 1.15. Let G be a group. Then a subgroup $Z \subseteq G$ is the *center* of G iff it consists of all the elements of G which commute with all other elements of G.

Definition 1.16. Let G be a group, and S be a G-set. Then the *orbit* of an element $s \in S$ is

$$Gs = \{g \cdot s \,|\, g \in G\} \tag{1.23}$$

The *stabilizer* of $s \in S$ is

$$G_s = \{g \in G \,|\, g \cdot s = s\} \tag{1.24}$$

Proposition 1.12. *The orbits of a group G on a G-set S form a partition of S.*

Theorem 1.6. *Suppose p is prime, and p divides the order of a group G. Then there exists $a \in G$ such that the order of a is p.*

Proof. Proceed by induction on the order of groups. First we prove the theorem for G abelian. Pick an element g of prime order q. We know this element exists since any element has order dividing $|G|$, and if g has order mn, $|g^m| = n$. If $q = p$ then we are done. If $q \neq p$ look at $G/\langle g\rangle$ which is of order $|G|/q \leq |G|$ which is divisible by p. As such, $G/\langle g\rangle$ falls under our inductive hypothesis, and has an element h of order p. Now we lift h to some $a \in G$. Then we know $a^p \in \langle g\rangle$ so a has order p, or pq. This means a or a^q has order p. Then we are done for Abelian G.

If G is not abelian, we look at the adjoint action of G on itself:

$$g \cdot s = gsg^{-1} \tag{1.25}$$

Now decompose G into orbits under conjugation. If a, b are in the same orbit, this means $a = gbg^{-1}$ for some $g \in G$. Since Lagrange's theorem tells us that the order of the orbit is the order of the group divided by the order of the stabilizer of the orbit at one point, we have that $|\text{orbit}| = |G|/|H|$. Since these orbits form a partition of G, we can write

$$|G| = \sum_{\text{orbits}} |\text{orbit}| = \sum_{\text{orbits}} |G|/|H| \tag{1.26}$$

We now have two different cases for H.

Case 1: There is some $H \subset G$ such that $|H| < |G|$ has order divisible by p. Then by induction, H has an element of order p, so G does as well.

Case 2: If $H \subset G$ such that $|H|$ is not divisible by p, then $|G| / |H|$ is divisible by p, so

$$\begin{aligned} |G| &= \sum_{\text{orbits } |H|<|G|} |G| / |H| + \sum_{\text{orbits } |H|=|G|} |G| / |H| & (1.27) \\ &= \sum_{\text{orbits } |H|<|G|} |G| / |H| + \sum_{\text{orbits } |H|=|G|} 1 & (1.28) \end{aligned}$$

The last sum is over elements g with $gh = hg$ for all $h \in G$. We recognize this as the center of G, which is abelian, and has order divisible by p, so it has element of order p from the first case. We also already know the first term is divisible by p, so we are done. □

Example 1.13. The previous theorem need not apply for nonprive divisors. For example, consider the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which has no element of order 4 but 4 divides the order of G

Definition 1.17. Let A, B be two normal subgroups of a group G. The *direct product* of A, B is the cartesian product with componentwise multiplication:

$$(a_1, b_1)(a_2, b_2) \coloneqq (a_1 a_2, b_1 b_2) \tag{1.29}$$

as inherited from G.

Proposition 1.13. *The direct product commutes.*

Proof. If A, B are two normal subgroups, then they commute with one another. □

Definition 1.18. Let A be a normal subgroups of a group G. Let B be another subgroup of G, which is not necessarily normal. For each $b \in B$ the map $a \mapsto bab^{-1}$ is an automorphism of A. Then if we write each such automorphism as φ_b for $b \in B$, then take $\varphi_{b_1}\varphi_{b_2} \coloneqq \varphi_{b_1 b_2}$ for $b_1, b_2 \in B$, so we have a homomorphism from B to $\mathrm{Aut}(A)$. The *semidirect product* of A and B, written

$$A \rtimes B \tag{1.30}$$

is then the cartesian product of the sets A, B equipped with the operation:

$$(a, b)(a', b') \coloneqq (a\, \varphi_b(a'), bb') \tag{1.31}$$

Remark 1.4. In other words, if we have an action of a non-normal subgroup B on a normal subgroup A, we can define the semidirect product $A \rtimes B$. We use this primarily to construct groups of a given order.

Example 1.14. We now proceed to classify the groups of order 6. Suppose G has order 6. Pick an element g of order 3. We know that: $\left\langle g, g^3 \right\rangle$ is a subgroup of order 3. We also know it is normal since it has index 2. Now pick an element $h \in G$ order 2, this gives the subgroup $\langle h \rangle$ which is not necessarily normal. This means G is the semidirect product of these subgroups of orders $2, 3$.

Consider $A = \mathbb{Z}/3\mathbb{Z}$ and $B = \mathbb{Z}/2\mathbb{Z}$ and an order 3 automorphism of A. We then have two possible actions of B on A. Namely, the identity, and $a \mapsto -a$. Then either $\varphi_b(a) = a$ or $\varphi_b(a) = -a$ for $b \neq e$. The first produces $\mathbb{Z}/6\mathbb{Z}$, and the second produces S_3. Then this gives us our 2 desired groups of order 6.

1.3.3 Exact sequences

Definition 1.19. Let A, B, C be groups, such that we have

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{1.32}$$

This is called an *exact sequence* iff the $\operatorname{im}(f) = \ker(g)$. An exact sequence is a *short exact sequence* iff it is of the form:

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1 \tag{1.33}$$

Example 1.15. Let G be a group, and H be a subgroup. Then consider the following exact sequence:

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1 \tag{1.34}$$

Be wary of the following blunder:

Warning 1.1. It is tempting to guess that G is either the direct product or the semi-direct product of H and G/H. This is however incorrect.

Example 1.16. Consider the short exact sequence:

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\text{inj}} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\text{surj}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \tag{1.35}$$

This shows that the blunder outlined in the previous example is indeed a blunder.

Example 1.17. The following is a common problem. Given A, B find G such that

$$1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1 \tag{1.36}$$

is a short exact sequence. The group G is called the extension of B by A (or sometimes the extension of A by B). This problem is hard even when A, B are abelian.

1.4 Groups of order 8

Remark 1.5. The careful reader might notice that we have missed groups of order 7. The more careful reader might have noticed that every group of order 7 is isomorphic to $\mathbb{Z}/7\mathbb{Z}$ by corollary 1.1.

Example 1.18. There are two cases of groups of order 8.

1. All elements have order 2. This implies the group is abelian, so it is really a vector space over F_2, and is isomorphic to $F_2 \times F_2 \times F_2$.

2. Some element have order 4 Then $H = \langle 1, g, g^2, g^3 \rangle$ is a subgroup of index 2, so it is normal. We write a corresponding exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/4\mathbb{Z} \arrow[r, "inj"] \arrow[d, equal] & G \arrow[r, "surj"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
 & H & & G/H &
\end{tikzcd} \tag{1.37}$$

Proposition 1.14. *The only groups of order* 8 *are* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$*,* $\mathbb{Z}/8\mathbb{Z}$*, the quaternion group* Q*, and the dihedral group* D_8*.*

Proof. We seek to classify all groups of order 8. Let G be a group of order 8. If G has all elements of order 2, then we have $(\mathbb{Z}/2\mathbb{Z})^3$. Alternatively, we have some g of order 4, so we have the subgroup $H = \langle g \rangle$ has index 2 and is therefore normal. Now pick some $h \in G$ mapping to a non-trivial element in $G/H = \mathbb{Z}/2\mathbb{Z}$. Then G contains $g, h, g^4 = e$ and h^2 which is e, g^{-1} or g^2. Note that $g^3 = g^{-1}$. Then since H is normal, hgh^{-1} is either g or g^3. Note that G is abelian iff $hgh^{-1} = g$. Therefore the non-abelian cases correspond to $hgh^{-1} = g^3 = g^{-1}$.

If $h^2 = g$ and $hgh^{-1} = g$, then $G \cong \mathbb{Z}/8\mathbb{Z}$. Otherwise, for abelian G, we could either have $h^2 = e$ or $h^2 = g^2$. If $h^2 = e$, we just get

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong F_2 \times F_2 \times F_2 \tag{1.38}$$

If $h^2 = g^2$, we have $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now we consider the non-abelian cases. If $hgh^{-1} = g^3$ then either $h^2 = g^2$ or $h^2 = e$. In the former case, we have the quaternion group Q, and in the latter we get the dihedral group D_8. We can't have $hgh^{-1} = g^3$ and $h^2 = g$, because then we have that G is simultaneously abelian and non-abelian. These results are summarized in the table below:

	$h^2 = e$	$h^2 = g$	$h^2 = g^2$
Abelian:	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Non-Abelian:	D_8	–	Q

□

1.4.1 Dihedral Group

Example 1.19. We consider a motivating example. A chess board is a board with 8×8 squares. How many ways can we position 8 non-attacking rooks on a chess board? In other words, how many ways can we choose 8 squares such that none share a row or column. The answer is

$$8 \times 7 \times \cdots \times 2 \times 1 = 40320 \tag{1.39}$$

What if we asked the same question up to symmetry? Let us consider D_8. This is the group of symmetries of a square. It acts on a set of 40320 elements. Then answering this question is the same as finding the number of orbits.

Theorem 1.7 (Burnside)**.** *Suppose there is some finite group G which acts on a set S. Then the number of orbits is equal to the average number of fixed points.*

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |S^g| \tag{1.40}$$

where S/G denotes the collection of orbits, and S^g is the set of elements of S fixed by g.

Proof. We look at the set of pairs with $g \cdot s = s$, and count this in two ways. First, for each g, there are $|S^g|$ choices for s so we get $\sum_{g \in G} |S^g|$ pairs.

Secondly, we look at each orbit of G on S. Say the orbit contains some $s \in S$. Then we know the number of points in the orbit is $|G| / |G_s|$. So this means $|G|$ is the size of an orbit times the number of elements of G fixing a point of the orbit. In other words,

$$\begin{aligned} |\text{pairs } (g,s)| &= \sum_{\text{orbits}} |\{\text{pairs in the orbit}\}| && (1.41) \\ &= \sum_i |Gs_i| \, |G_{s_i}| && (1.42) \\ &= |G| \, |S/G| && (1.43) \end{aligned}$$

where the index i runs over representatives s_i of distinct orbits. Then we divide by $|G|$ and we are done. □

Definition 1.20. Let G be a group. Two elements $a, b \in G$ are *conjugate* iff there is some $g \in G$ such that $a = gbg^{-1}$.

Remark 1.6. Intuitively, two elements of a group are conjugate if they “look” the same.

Example 1.20. In the group D_8, we have that the elements of the group which are conjugate all give the same number of fixed points. This is the sense in which conjugate elements “look” the same. In particular, a horizontal flip is the same as a $\pi/2$ clockwise rotation, followed by a vertical flip and a $\pi/2$ counter-clockwise rotation. A reflection over both diagonals is the same as a vertical flip, a $\pi/2$ clockwise rotation, and an inverted vertical flip. All together we have:

Element	Number of configurations fixed
identity	$8! = 40320$
vertical, horizontal flip	$2 \times 0 = 0$
reflect along both diagonals	$8 \times 6 \times 4 \times 2 = 384$
$\pi/2$ rotation	$2 \times (6 \times 2) = 24$
reflect along one diagonal	$2 \times 764 = 1528$
Total:	42256

Now we can finally calculate the number of ways to arrange the rooks up to symmetry. For the case where we flip both corners, there are 8 possibilities for row 1, then there are 6 for row 2, then 4, then 2.

For the bottom row, we use c_n to denote the number of ways to arrange n rooks on an $n \times n$ board invariant under corner to corner flip. For the first possibility, we take the top left corner. Then c_{n-1} ways to arrange others. The second possibility, is that we choose a non-corner, which restricts the flipped position, and leaves c_{n-2} ways to choose others. This means $c_{n-1} + (n-1)\, c_{n-2} = c_n$. We can solve this for $c_8 = 764$.

n	1	2	3	4	5	6	7	8
c_n	1	2	4	10	26	76	232	764

Now we have the sum is 42256, so by the above theorem, up to symmetry we can arrange the rooks $42256/8 = 5282$ ways.

Warning 1.2. Note that we write D_{2n} for the group of symmetries of the regular n-gon, meaning there are n rotations and n reflections, giving us a group of order $2n$. Some sources will instead write D_n.

1.4.2 Quaternions

Definition 1.21. The quaternion group consists of 8 elements: $\pm 1, \pm i, \pm j, \pm k$ where

$$ij = -ji = k \tag{1.44}$$

$$ji = -ik = j \tag{1.45}$$

$$jk = -kj = i \tag{1.46}$$

$$i^2 = j^2 = k^2 = -1 \tag{1.47}$$

Proposition 1.15. *The elements of the quaternions can also be written:*

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{1.48}$$

Definition 1.22. The quaternion[1.3] numbers are given by

$$\{a + bI + cJ + dK \mid a, b, c, d \in \mathbb{R}\} \tag{1.49}$$

where we have a notion of conjugation given by:

$$z = a + bI + cJ + dK \qquad \bar{z} = a - bI - cJ - dK \tag{1.50}$$

Proposition 1.16. *The quaternion numbers contain* $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$.

Proposition 1.17. *The quaternion numbers form a* 4*-dimensional division algebra*[1.4] *containing* $\mathbb{C}$. *The non-zero quaternions form a group under multiplication.*

Proof. Key Point: any non-zero quaternion has an inverse. This is like a generalized complex number. We have notions of conjugation as well. Namely for $z = a + bI + cJ + dK$ we have:

$$\bar{z} \coloneqq a - bI - cJ - dK \tag{1.51}$$

so we get that $z\bar{z} = a^2 + b^2 + c^2 + d^2$

Note we can now write that

$$z^{-1} = \frac{\bar{z}}{z\bar{z}} \tag{1.52}$$

This means non-zero quaternions form a group under multiplication. Note that the quaternion group is a subgroup of the non-zero quaternions. □

Proposition 1.18. *The quaternion group is a subgroup of* S^3.

Proof. Note that we have a homomorphism from the nonzero quaternions $\mathbb{H}^\times \to \mathbb{R}^\times$ given by

$$z \mapsto |z| \tag{1.53}$$

In addition, the kernel of this map is

$$S^3 = \left\{z : a^2 + b^2 + c^2 + d^2 = 1\right\} \tag{1.54}$$

Therefore we have

$$\{\pm 1, \pm I, \pm J, \pm, K\} \subseteq S^3 \tag{1.55}$$

as desired. □

Remark 1.7. Note this is the same story as $\mathbb{C}$ only in higher dimensions. This only works for S^0, S^1, S^4.

Definition 1.23. The set of matrices $SO_3(\mathbb{R})$ is the *special orthogonal group* iff it consists of all rotations in $\mathbb{R}^3$. Explicitly these are transformations that preserve the origin, euclidean distance, and orientation.

[1.3] The word quaternion actually means soldier. Quaternions are referenced in this sense in the New Testament.

[1.4] See definition 3.11.

Proposition 1.19. *If we choose an orthonormal basis for $\mathbb{R}^3$, the elements of* $\mathrm{SO}_3(\mathbb{R})$ *can be given by the orthogonal matrices with determinant* 1.

Proposition 1.20. *Conjugation by an element of $\mathbb{H}^\times$ gives a homomorphism* $S^3 \to \mathrm{SO}_3(\mathbb{R})$.

Proof. Identify the following:

$$\mathbb{R}^3 = \{bI + cJ + dK\} \subseteq \mathbb{H} \tag{1.56}$$

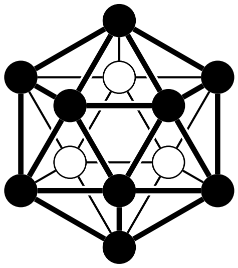
Then for $g \in \mathbb{H}^\times$, the map $v \mapsto g^{-1}vg$ maps $\mathbb{R}^3 \to \mathbb{R}^3$. Note the above map preserves $|v|$. It is in fact a rotation[1.5], and we therefore get a homomorphism $S^3 \to \mathrm{SO}_3(\mathbb{R})$. This is not quite an isomorphism because the kernel is of order 2. Explicitly it is $\{\pm 1\}$. So we get

$$1 \longrightarrow \{\pm 1\} \longrightarrow S^3 \longrightarrow \mathrm{SO}_3(\mathbb{R}) \longrightarrow 1 \tag{1.57}$$

So S^3 is "off" by 2. □

Example 1.21. Any finite group of rotations in $\mathrm{SO}_3(\mathbb{R})$ is an example of this same phenomenon. In particular, in $\mathbb{R}^3$, consider the rotations of a rectangle: $(\mathbb{Z}/2\mathbb{Z})^2$. The pre-image of this under the previous homomorphism has twice the order of the group, and yields the quaternions.

Example 1.22. Consider the rotations of an icosahedron. This has 60 elements. However, the inverse image of the previous homomorphism is a subgroup of S^3 of twice the other.



This yields the binary icosahedral group, of order 120.

1.5 Groups of order p^2

Proposition 1.21. *There are only two abelian groups of order* 9*:*

$$\mathbb{Z}/9\mathbb{Z} \qquad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \tag{1.58}$$

[1.5] Quaternions are sometimes used to calculate rotations in computer graphics, since they are faster to work with than matrices.

Proof. These two group clearly have order 9. These are also the only abelian groups of this order, because if we have an element of order 9 then we must have $\mathbb{Z}/9\mathbb{Z}$. If we have an element of order 3 then it is abelian, and isomorphic to a vector space over F_3. This takes a bit of effort to prove, but all vector spaces are isomorphic.

$$F_3 \times F_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \tag{1.59}$$

□

What about non-abelian groups of order 9? To examine this, we will prove that all groups of order p^2 for prime p are abelian.

Definition 1.24 (Center)**.** Given a group G, the *center* of G is a subgroup of G consisting of all of the elements of G which commute with all the other elements of G.

Lemma 1.3. *Any group of order p^n for $n \geq 1$ has a non-trivial center.*

Proof. We look at conjugacy classes of G. Let C_g denote the conjugacy class of an element $g \in G$. Take some $g \in C_g$ for each C_g. Then each conjugacy class of G corresponding to g has size equal to the order of G divided by the elements fixing g. We call the center Z, and write:

$$|G| = \sum_g |C_g| = \sum_g \frac{|G|}{|G_g|} = \sum_{g \notin Z} \frac{|G|}{|G_g|} + |Z| \tag{1.60}$$

Note that the conjugacy classes are the orbits under adjoint action $g \cdot h = ghg^{-1}$. Now we have two possibilities. The first is that g is in the center and the size of the conjugacy class is 1. Otherwise it is not in the center, in which case the conjugacy class has order divisible by p (actually it is a power of p). So the number of conjugacy classes of size 1 is divisible by p. The key point here is that p divides the order of the center, and therefore it has at least p elements, and is non-trivial as desired. □

Remark 1.8. In general it is very hard to find elements of the center, so it is nice that this weird counting argument gives lemma 1.3.

Theorem 1.8. *Every group of order p^2 is abelian.*

Proof. Suppose $|G| = p^2$. By the previous lemma we know the center Z cannot have order 1, so it must have order p or p^2. Since p^2 implies it is equal to the entire group, we want to show that $|Z| = p$ is not possible.

Suppose $g \notin Z$. If $g^2 \in Z$, then g has order p^2, and generates all of G. Then assume $g^2 \notin Z$, so $\langle g \rangle \cap Z = \{e\}$. Then $G = \langle g \rangle Z$ so every element of G can be written $g^m a$ for some $m \in \mathbb{Z}$, and $a \in Z$. Therefore the order of the center is p^2 which means $G = Z$ and G is abelian as desired. □

Remark 1.9. Note that the proof of theorem 1.8 is a special case of the more general fact that if Z is the center of a non-abelian group G then G/Z not cyclic.

Remark 1.10. This means we have classified all groups of order p^2 for prime p. We only ever have:

$$\mathbb{Z}/p\mathbb{Z}^2 \qquad\qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \tag{1.61}$$

1.6 Nilpotent groups

Example 1.23. Suppose we have a group G_0 of order p^n for $n \geq 0$. Then we assign Z_0 to be the center of that group. Now set $G_1 = G_0/Z_0$ and call the center of this new group Z_1. Then if we continue this until the group has order 1, then killing the center doesn't make it any smaller.

Definition 1.25. A group is called *Nilpotent* if it can be reduced to one element by killing the center repeatedly.

Example 1.24. It might seem that this is a silly process, and killing the center once will typically be enough to get rid of the "abelian" bits. To see this is not the case, consider:

$$G = \{\pm 1, \pm I, \pm J, \pm, K\} \qquad\qquad Z = \{\pm 1\} \tag{1.62}$$

Then $G/Z = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ which has a non-trivial center itself.

Proposition 1.22. *All groups of order p^n are nilpotent. Furthermore all products of groups of prime order are nilpotent.*

Proof. All such groups of order p^n have non-trivial center, and never acquire a trivial center, since they are repeatedly of prime power order. □

Remark 1.11. Almost all nilpotent groups are boring. There are many groups of order p^n for example...

Remark 1.12. We shall eventually see a form of the converse: any finite nilpotent group is a product of groups of order p^n. For more, see theorem 1.10.

1.7 Groups of order $2p$

Example 1.25. We motivate the general statements with the example of groups of order 10. We can in fact recall the methods used in section 1.3.2 to get groups of order $2p$ for prime p. In particular, for a group G, we find a subgroup H of order p. Then H has index 2 so it is normal. Then we can choose an element a of order 2 so we get $\langle a \rangle$ is a subgroup of order 2, and the groups of this order can be classified by the ways $\langle a \rangle$ can act on H to form $H \rtimes \langle a \rangle$.

Theorem 1.9. *All groups of order $2p$ for prime p are of the form*

$$H \rtimes \mathbb{Z}/2\mathbb{Z} \tag{1.63}$$

for H normal of order p.

Proof. Automorphisms of $\mathbb{Z}/p\mathbb{Z}$ are just given by nonzero elements of $\mathbb{Z}/p\mathbb{Z}$. In particular, we can just take $1 \mapsto$ any non-zero element. Then the group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is cyclic of order $p-1$. In addition, the only elements of order 2 are ± 1. As such, there are 2 groups of this order. If the group is abelian, we have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Otherwise we get the dihedral group, which consists of the symmetries of the regular p-gon. □

Example 1.26. For order 10, D_{10} is the symmetries of the pentagon.

1.8 Groups of order 12

We have the following groups of order 12:

- $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $D_{12} \cong D_6 \times \mathbb{Z}/2\mathbb{Z}$ (non-abelian)
- Rotations of tetrahedron: A_4 (non-abelian)
- Binary dihedral group (non-abelian)

1.8.1 Dihedral, binary dihedral groups

Proposition 1.23. *For any $n \in \mathbb{N}$, the group D_{8n+4} can be split into the product $D_{4n+2} \times \mathbb{Z}/2\mathbb{Z}$.*

Example 1.27. As we have seen, $D_{12} = D_6 \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 1.24. *If we have a homomorphism $S^3 \to \mathrm{SO}_3(\mathbb{R})$ then inverse image of some group $G \subseteq \mathrm{SO}_3(\mathbb{R})$ is a subgroup of S^3 of order $2 \times |G|$.*

Proposition 1.25. *The binary dihedral group is a group of order 12.*

Proof. This is the lift of D_6 from $\mathrm{SO}_3(\mathbb{R})$ to S^3 and therefore has order 12. □

Remark 1.13. “Binary” typically means a lift from $\mathrm{SO}_3 \to S^3$.

1.8.2 Rotations of tetrahedron

Example 1.28. For example, S_3 is the symmetries of a triangle in 3-d and has order 6. This yields A_4 under the previous map. We can recognize this as the rotations of the tetrahedron, since it has $4 \times 3 = 12$ items. The conjugacy classes are:

Element	Order
Identity	1
Rotation by $2\pi/3$	4
Rotation by $4\pi/3$	4
Reflect across opp. edges	3
Total:	12

But how do we know if we have all groups of order 12? We resort to the Sylow theorems…

1.8.3 Sylow theorems

If $H \subseteq G$ then the order of H divides the order of G by Lagrange, but what about the converse? This is not the case in general, but it is the case in some particular cases.

Example 1.29. As a counterexample to the converse of Lagrange's theorem, consider that A_4 has no subgroup of order 6.

Theorem 1.10 (Sylow)**.** *Suppose p^n divides $|G|$ and p^{n+1} does not divide $|G|$. Then we have that*

1. *There exists a subgroup of order p^n.*
2. *All sylow subgroups are conjugate.*
3. *The number of p-sylow subgroups of G is $\equiv 1 \pmod{p}$.*
4. *Any subgroup of order p^m for $m \leq n$ is contained in some p-sylow subgroup.*

Proof. (1): We have two cases to treat, then we proceed by induction on $|G|$. Either some proper subgroup has index prime to p or the index of every proper subgroup is divisible by p. In the first case, we than have that p divides $|H|$ so H has a subgroup of order p^n by induction. In the second case all proper subgroups have index divisible by p. Consider the action of G on itself. Then if the stabilizer is the whole of G, any orbit of G has 1 element. Otherwise the stabilizer of points is not equal to G. Then the number of elements is a multiple of p. We know that

$$|G| = \sum_i C_{g_i} \tag{1.64}$$

where C_g denotes the conjugacy class of g, and i ranges over the distinct conjugacy classes. Then since the order of the group is divisible by p, it must be the case that the sum in (1.64) is divisible by p or consists of one element in the center. So the order of the center is divisible by p as we have seen.

Now pick g in the center divisible by p. Then $G/\langle p\rangle$ has subgroup order p^{n-1} by induction, since g is in the center. This shows that the inverse image of subgroup has order p^n.

See Lang [5] for $(2), (3), (4)$. □

Proposition 1.26. *The five groups of order* 12 *that we have already listed, are the only groups of order* 12.

Proof. We now apply the Sylow theorems to groups of order 12. First look at subgroups of order 3. The number of these subgroups is $1 \bmod 3$ and divides 12 as well. Then there are only two possibilities: 1 and 4.

If there is only one subgroup of order 3, it must be normal. It also must then have a subgroup of order $2^2 = 4$. Therefore $G = A \times B$ where A is normal of order 3, and B of order 4.

Action on:	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Trivial	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Non-Trivial	Binary Dihed	$D_{12} = D_6 \times \mathbb{Z}/2\mathbb{Z}$

Note the trivial action yields an abelian group, and a non-trivial action gives a non-abelian group.

Now returning above, we take the case of 4 subgroups of order 3. We can identify the four subgroups of order 3 as vertices with three elements connecting the vertex to the other vertices. Let us call these A_1, A_2, A_3, A_4 where $A_i \cap A_j = \{e\}$ if $i \neq j$. This means we get $4 \times 2 = 8$ elements of order 3 which leaves 4 elements not of order 3. But we know that there exists a subgroup of order 4 from the Sylow theorems, so it must consist exactly of elements not of order 3. So $G = X \rtimes Y$ where X is normal of order 4 and Y is of order 3. So $\mathbb{Z}/3\mathbb{Z}$ is this subgroup of order 4. This implies that $G = A_4$, the rotations of a tetrahedron. □

1.8.4 Solvability

Remark 1.14. We have seen that every group of order ≤ 12 can be split up into cyclic groups. This is a rough notion of solvability. More formally:

Definition 1.26 (Solvable)**.** Let G be a group. Then it is *solvable* iff it is either cyclic, or it has a normal subgroup N such that G/N is solvable.

Definition 1.27 (Simple)**.** A group G is *simple* iff it has no non-trivial normal subgroups.

Example 1.30. The group $\mathbb{Z}/p\mathbb{Z}$ is simple for all prime p.

Example 1.31. We now provide an example of a non-cyclic simple group.

Consider the rotations of an icosahedron:

Element	Order	Number	Description
Identity	1	1	
Rotation by $2\pi/3$	3	20	one for each face
Rotation by $4\pi/3$	–	–	same as $2\pi/3$ (opposite face)
Rotation by $2\pi/5$	5	12	each corresponding to vertex
Rotation by $4\pi/5$	5	12	each corresponding to vertex
Rotation by $6\pi/5$	–	–	same as $2\pi/5$ (opposite corner)
Rotation by π	2	30/2	bring edge to opposite edge
Total		60	

Note for the rotation by π, we have two edges corresponding to every action, which gives us the factor of two.

Any normal subgroup must be the union of conjugacy classes, since unions are closed under conjugation. Now suppose n is the order of the normal subgroup. Then n must be 1 plus some of $\{12, 12, 15, 20\}$. But n must also be a divisor of 60:

$$1, 2, 3, 5, 6, 10, 12, 15, 20, 30, 60 \tag{1.65}$$

The only possibilities are: $1 = 1$ or $1 + 12 + 12 + 15 + 20 = 60$. As such, the normal subgroups have orders $1, 60$.

Theorem 1.11 (Jordan Hölder)**.** *Let G be a group with a normal decomposition which eventually reaches the trivial group. Then the simple groups we get are independent of splitting choice.*

Proof. See Lang. [5].[1.6] □

Remark 1.15. Finite simple groups have been classified as 18 types in infinite series and 26 others (sporadic).

Example 1.32. The group $\mathrm{GL}_n(\mathbb{F}_n)$ is not always simple. To see this, consider the determinant map: $\det : \mathrm{GL}_n \to \mathbb{F}_p^\times$. Notice the kernel of this map is normal. If we then quotient out by this to get $\mathrm{SL}_n(\mathbb{F}_p)$, and then quotient out by the center, we get:

$$\mathrm{PSL}_n(\mathbb{F}_p) = \mathrm{SL}_n/\mathbb{Z} \tag{1.66}$$

which is not always simple. Note: $\mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_3)$ are not simple but others are.

[1.6] Professor Borcherds said when he looked at the proof he stared at a picture of a butterfly for a while and gave up. He has never actually used it.

1.9 Groups of order $13-16$

Proposition 1.27. *There is only one group of order* 13*:* $\mathbb{Z}/13\mathbb{Z}$*. There are only two groups of order* 14*:* $\mathbb{Z}/14\mathbb{Z}$ *and* D_{14}*.*

Proof. Since 13 is prime, the group of this order is unique. Since $14 = 2 \times 7$ and 7 is prime, this is a group of order $2p$ which we have already classified as such back in section 1.3.2. □

1.9.1 Groups of order pq

Theorem 1.12. *If* G *is a group of order* pq *for* $p, q \in \mathbb{Z}$ *primes, then if* p *does not divide* $(q-1)$ *we have that* $G \cong \mathbb{Z}/pq\mathbb{Z}$*.*

If p *does divide* $q-1$*, we have that either* $G \cong \mathbb{Z}/pq\mathbb{Z}$ *or* $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$*.*

Proof. First take $p < q$. From the Sylow theorems we know there is some subgroup of order q, and the number of conjugate subgroups is $\equiv 1 \bmod q$ and divides pq. Since $p < q$, the only possibility is 1. Therefore G has a normal subgroup $\mathbb{Z}/q\mathbb{Z}$, so G is the semi-direct product of $\mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$.

We know $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^*$ is of order $q-1$. This is also cyclic, so has subgroup of order p if p divides $q-1$. So now we have two cases. Either p does or does not divide $q-1$. If it does not, the only subgroup of order pq is cyclic. If it does divide $q-1$ then we get two possibilities: cyclic $\mathbb{Z}/pq\mathbb{Z}$ or the semi-direct product of $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. □

Example 1.33. There is only one group of order 15.

Example 1.34. For $p = 2$, 2 divides $q-1$ so we get the cyclic and dihedral groups.

Example 1.35. For order 21, we have that $3|7-1$ so we get a non-abelian group. This is the smallest non-abelian group of odd order.

1.9.2 Groups of order 16

Remark 1.16. These groups are quite messy. In general $p^n, n \geq 4$ and p prime are pretty messy. . . We have 14 in total.

Proposition 1.28. *The following are the abelian groups of order* 16*.*

1. $\mathbb{Z}/16\mathbb{Z}$
2. $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
3. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
4. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5. $(\mathbb{Z}/2\mathbb{Z})^4$

Proposition 1.29. *The following are non-abelian groups of order* 16 *with an element of order* 8*:*

group	*identity*	*conjugation*	
gen. Q	$g^8 = e$	$aga^{-1} = g^{-1}$	$a^2 = g^4$
dihedral	$g^8 = e$	$aga^{-1} = g^{-1}$	$a^2 = 1$
semidihedral	$g^8 = e$	$aga^{-1} = g^3$	$a^2 = 1$
nameless	$g^8 = e$	$aga^{-1} = g^5$	$a^2 = 1$

Proposition 1.30. *The groups of order* 16 *which are formed as products (or semidirect product) are as follows:*

- $\mathbb{Q}_8 \times \mathbb{Z}/2\mathbb{Z}$
- $D_8 \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
- $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/4\mathbb{Z}$

Proposition 1.31. *The Pauli matrices also generate a group of order* 16*:*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.67}$$

1.10 Finitely Generated Abelian Groups

All of the finitely generated abelian groups that we have seen so far have been finite products of $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ and $\mathbb{Z}$. As it turns out, groups of this form are the only examples.

Theorem 1.13. *Let G be a finitely generated abelian group. Then G is a finite product of groups of the form $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$.*

Proof. Suppose G is an abelian group generated by $g_1, \ldots, g_n$. We write the general generating relations as follows:

$$\begin{aligned} m_{11}g_1 + \quad \ldots + m_{1n}g_n = \quad & 0 \qquad (1.68) \\ m_{21}g_1 + \quad \ldots + m_{2n}g_n = \quad & 0 \qquad (1.69) \\ \ldots \qquad \ldots \qquad & \ldots \qquad (1.70) \end{aligned}$$

so we have a possibly infinite matrix of coefficients. We now can use the following operations to get it in a more comfortable form:

- Add $k\times$ any column to any other column. This corresponds to changing generators. Explicitly $g_i \to g_i + kg_j (i \neq j)$

- Add $k\times$ any row to any other row. This is allowed since if rows $r = s = 0$ then $k \times r + s = 0$.

We can do these an infinite number of times. We apply these to make $m_{11} > 0$ as small as possible. We then subtract column 1 from the other columns to make row 1 have all other entries be zero. The point here is that m_{11} divides m_{12}. If this were not the case, then we can just replace m_{11} by the remainder. Then the remainder would be a candidate for m_{11} as well by construction, and this contradicts the fact that m_{11} was minimal. Formally, $m_{12} = km_{11} + r$ for $|r| < m_{11}$ so we can just subtract km_{11} from m_{12} and then subtract $r = m_{12}$ from m_{11} to make m_{11} smaller.

Now repeat this to kill every column. Now we are left with only the diagonal M_{ii}. We can assume they are all non-negative. This means G is generated by $\{g_i\}$ with relations $m_{ii}g_i = 0$. Therefore we can write that

$$G \simeq \mathbb{Z}/m_{11}\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{nn}\mathbb{Z} \tag{1.71}$$

as desired. □

Remark 1.17. The decomposition constructed in the previous proof is not unique as it stands. It is however unique if we insist that either $m_{11}|m_{22}\dots$ or if we insist that all m_{ii} are either prime powers or 0. Then this gives us uniqueness up to order.

1.11 Groups of order $17 - 24$

Proposition 1.32. *There is only one group of orders* $17, 19$ *and* 23.

Proof. The numbers $17, 19, 23$ are prime so this follows from corollary 1.1. □

Proposition 1.33. *There are* 5 *groups of order* 18 *given by semidirect products.*

Proof. Every group of order 18 has a normal subgroup of order 3^2 or 5. Then we can classify the semidirect products to get 5 different groups. □

Proposition 1.34. *There are* 5 *groups of order* 20 *given by semidirect products.*

Proof. Groups of order 20 have a normal subgroup of order 5. We can then classify the groups by semidirect products to get 5 groups, as in the case of order 18. □

Proposition 1.35. *The only abelian group of order* 21 *is* $\mathbb{Z}/21\mathbb{Z}$. *There is also a non-abelian group of order* 21.

Proof. This falls under the pq case for $p = 3$ and $q = 7$. Then $3|6 = 7-1$ so the result follows from the classification of groups of order pq in section 1.9.1. □

Proposition 1.36. *The only two groups of order* 22 *are* D_{22} *and* $\mathbb{Z}/22\mathbb{Z}$.

Proof. Since $22 = 2 \times 11$ and 11 is prime we have that this falls under the classification of groups of order $2p$. □

Example 1.36. The group S_4 and the binary tetrahedral group are of order 24. Note the binary tetrahedral group is the inverse image of A_4 under the usual map from $S^3 \to \mathrm{SO}_3$. There are a dozen or so other groups of order 24…

1.12 Symmetric Group

1.12.1 Definitions, examples

Definition 1.28. The *symmetric group* S_n is the group of all permutations of n elements.

Proposition 1.37. *Let S_n be as in definition 1.28. Then $|S_n| = n!$.*

Proof. There are n choices for the image of 1, $n-1$ choices for the image of 2 etc. □

Definition 1.29. A *cycle* $\left(a\,b\,c\right)$ is a function bring $a \mapsto b \mapsto c \mapsto a$.

Example 1.37. We can concatenate cycles such as $\left(1\,2\,3\right)\left(4\,7\,6\right)\left(5\,4\right)$.

Definition 1.30. A cycle is a *transposition* iff it exchanges 2 elements and leaves all the others.

Proposition 1.38. *The transpositions generate S_n. In other words, we can get any permutation by swapping adjacent elements.*

Proof. Bubble sort[1.7] is a sorting algorithm which works by swapping adjacent elements until it reaches the desired order. It takes $n\left(n-1\right)/2$ changes in the worst case. □

1.12.2 Alternating group

Example 1.38. Look at S_n acting on $x_1, \cdots, x_n$. Then we can extend this action to $\mathbb{C}\left[x_1, \cdots, x_n\right]$. Now consider the discriminant[1.8]:

$$\Delta = (x_1 - x_2)\cdots(x_1 - x_n)\cdots(x_2 - x_2)\cdots(x_{n-1} - x_n) = \prod_{i<j}(x_i - x_j) \quad (1.72)$$

Now notice that any $\sigma \in S_n$ either maps $\Delta \mapsto \Delta$ or $\Delta \mapsto -\Delta$. In other words for $n \geq 2$ we have an homomorphism

$$\epsilon : S_n \to \{\pm 1\} \quad (1.73)$$

such that

$$\sigma\Delta = \epsilon\left(\sigma\right)\delta \quad (1.74)$$

[1.7] bogosort is the worst sorting algorithm. Bubble sort is second worst.

[1.8] We will see more about this in chapter 4 on polynomials.

Definition 1.31. The *alternating group* is defined as follows:

$$A_n := \{\sigma \in S_n : \epsilon(\sigma) = 1\} \tag{1.75}$$

or equivalently that $\sigma\Delta = \Delta$. Note $A_n = \ker(\epsilon)$.

Proposition 1.39. *The group A_n is normal in S_n and of order $n!/2$ for $n \geq 2$*

1.12.3 Platonic Solids

Example 1.39. The symmetric and alternating groups apply conveniently to the rotations and reflections of the platonic solids. First consider the tetrahedron. The rotations and reflections of a tetrahedron comprise S_4 because we are looking at the permutations of the vertices. Then the rotations are just A_4. Next, the rotations of a cube/octahedron are given by S_4 acting on the permutations of the diagonals. The rotations and reflections are given by $S_4 \times \mathbb{Z}/2\mathbb{Z}$. The dodecahedron and icosahedron have their rotations given by an action on the 5 inscribed cubes. So we get a homomorphism of rotations to S_5. In particular this group is A_5. Then the rotations and reflections are given by the product $A_5 \times \mathbb{Z}/2\mathbb{Z}$. Note however that $A_5 \times \mathbb{Z}/2\mathbb{Z} \ncong S_5$. To take the product of A_5 with something to get S_5 somehow an element of order 2 must be put in the center. This is summarized in the following tables:

solid	faces	rotations	rotations and reflections
tetrahedron	4	$12 = \lvert A_4\rvert$	$24 = \lvert S_4\rvert$
cube, octahedron	$6, 8$	$24 = \lvert S_4\rvert$	$48 = \lvert S_4 \times \mathbb{Z}/2\mathbb{Z}\rvert$
Dodec., Icosa.	$12, 20$	$60 = \lvert A_5\rvert$	$120 = \lvert A_5 \times \mathbb{Z}/2\mathbb{Z}\rvert$

Note that -1 is not an automorphism of the top row. Also, in the bottom row, rotations map injectively into A_5, because the group of rotations is simple, so the kernel is all or nothing. The solids in the bottom two rows share rows because they can be “intertwined” nicely. “Spherical Reflection groups” are in the right column.

1.12.4 Conjugacy Classes

Definition 1.32. The *cycle shape* of an element of S_n is the multiplicity of cycles of each given size.

Example 1.40. Consider the element $\left(1\,2\,4\right)\left(5\,7\,8\right)\left(6\,9\right)\left(10\right)\left(3\right)$. This has cycle shape $3^2 21^2$.

Example 1.41. Consider elements $a, b \in S_n$ with the same cycle shape. How might we find g such that $a = gbg^{-1}$? In particular, let us consider:

$$\left(1\,2\,4\right)\left(5\,7\,8\right)\left(6\,9\right)\left(10\right)\left(3\right) \tag{1.76}$$

$$\left(2\,4\,5\right)\left(6\,7\,8\right)\left(1\,3\right)\left(9\right)\left(0\right) \tag{1.77}$$

These are expressed as products of disjoint cycles. The cyclic shape for both of them is $3^2 21^2$. The key point here is that 2 elements are in the same conjugacy class of S_n if they have the same cycle shape. The problem then is determining the element g such that $a = gbg^{-1}$. Notice we can express g in terms of transpositions by inspection of (1.76) and (1.77) by sending the bottom to the top. In other words:

$$g = (165421)\,(3910)\,(7)\,(8) \tag{1.78}$$

Example 1.42. Consider the group S_4. How many conjugacy classes do we have? This can be rephrased as the number of cycle shapes, which can be rephrased as the number of partitions of 4. If we take C_σ to be the conjugacy class of σ, and G_σ to be the stabilizer under conjugation (aka the centralizer) then we have the following chart, where S_4 is viewed as the rotations of a cube:

partition	cycle shape	$\lvert G_\sigma \rvert$	$\lvert C_\sigma \rvert$	C_σ
$1+1+1+1$	1^4	$4! = 24$	1	id
$2+1+1$	21^2	$2 \times 1! \times 1^2 \times 2! = 4$	6	rot. by $\pi/2$
$3+1$	31	$3 \times 1! \times 1! = 3$	8	rot. by $2\pi/3$
$2+2$	2^2	$2^2 \times 2! = 8$	3	rot. by π
4	4	$4 \times 1! = 4$	6	rot. by π

Notice the fourth column is $\lvert C_\sigma \rvert = \lvert G \rvert / \lvert G_\sigma \rvert$. In general, if σ has shape $1^{n_1} 2^{n_2} \cdots$ the number of elements in the centralizer is:

$$1^{n_1} n_1! 2^{n_2} n_2! \cdots \tag{1.79}$$

1.12.5 Normal subgroups of S_n

Remark 1.18. We now seek to find the normal subgroups of S_n. We already know $\{e\}, A_n, S_n$ are normal, but what about others?

Example 1.43. Take S_4, viewed as the rotation of a cube, to act upon the set of 3 lines joining opposite faces. This gives us a homomorphism from S_4(rotations of the cube) to S_3(permutations of 3 lines). In particular, the kernel of this map is a normal subgroup of order 4. This contains the identity, and three rotations by π. In S_4, recall the table from example 1.42. The 1st and 4th rows of this table form a normal subgroup, as do the 1st, 3rd, and 4th.

Following the same pattern, we have homomorphisms from S_2 onto S_1, from S_3 onto S_2, from S_4 onto S_3, but not from S_5 onto S_4. This is because A_5 is a simple subgroup of S_5. Recall A_5 is the group of rotations of an icosahedron. If N is any normal subgroup of S_5, $N \cap A_5$ is normal in A_5 so N is trivial or A_5. Therefore the only normal subgroups of S_5 are $\{e\}, A_5$, and S_5.

Theorem 1.14. *A_n is simple for all $n \geq 5$.*

Proof. Proceed by induction on n. Let $n \geq 5$, and suppose N is normal in S_n. Pick some $g \in N$, $g \neq 1$, and find h so that $ghg^{-1}h^{-1}$ fixes the point 1. Then

$$ghg^{-1}h^{-1} = g\left(hg^{-1}h^{-1}\right) \in N \tag{1.80}$$

This means N has a non-trivial intersection with S_{n-1} (the elements fixing 1) so $N \cap S_{n-1}$ is either A_{n-1} or S_{n-1} since A_{n-1} simple.

So N contains all elements of A_n fixing 1. Similarly, it contains all elements fixing i for any i. We leave it as an exercise to show that this generates A_n. □

Example 1.44. There are three groups of order 120 containing A_5 and $\mathbb{Z}/2\mathbb{Z}$ as composition factors.

1. $A_5 \times \mathbb{Z}/2\mathbb{Z}$
2. S_5: has subgroup A_5, quotient group $\mathbb{Z}/2\mathbb{Z}$
3. Binary icosahedral group: has quotient group A_5, Subgroup $\mathbb{Z}/2\mathbb{Z}$.

Note that $1, 2$ from above are semidirect products, and 3 is not. As one might guess from the word "binary," 3 from above is the inverse image of A_5 under the map $S^3 \to \mathrm{SO}_3(\mathbb{R})$. In addition, if G is the binary icosahedral group, then S_3/G gives the Poincaré 3-sphere which is not a group, but is still a topological space. It has the same homology as S^3 but is not homeomorphic.[1.9]

1.12.6 Automorphisms

Definition 1.33. Let G be a group. An inner automorphism of G is given by the conjugate action of some element of G. This yields the exact sequence:

$$\begin{aligned} 1 \longrightarrow Z \longrightarrow \ \text{conjugations} \ &\longrightarrow \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1 \\ g \longrightarrow (h \to ghg^{-1}) & \end{aligned} \tag{1.81}$$

where Out denotes the set of *outer automorphisms* which is the quotient Aut / Inn where Inn is the subgroup consisting of all inner automorphisms.

Proposition 1.40. $\mathrm{Aut}(S_n) \cong S_n$ *for* $n \geq 3$ *except when* $n = 6$. *All of these automorphisms are inner automorphisms.*

Remark 1.19. In general this is a typical occurrence with finite groups, that these types of statements hold for all but some annoying special cases.

Proof. We now find a non-inner automorphism of S_6. Start with S_5. The key points is that this has a subgroup of order 20. S_5 acts on $\{0, 1, 2, 3, 4\} = \mathbb{F}_5$, and has a subgroup consisting of all permutations of the form $x \to ax + b$ where $a, b \in \mathbb{F}_5$, so there are 20 elements.

[1.9] Homology might simply be said to count the n-dim holes in a manifold.

This means S_5 has subgroup of index $6 = 120/20$, so it acts transitively on 6 points. This gives us a homomorphism $S_5 \to S_6$ which is different from the usual such non-transitive homomorphisms, which fix some element. It is clear that since there is a point fixed it is therefore not transitive. So S_6 has 12 subgroups isomorphic to S_5, rather than 6 of them as we might expect.

This constructed subgroup of S_6 is therefore a homomorphism from $S_5 \to S_6$. Any subgroup of index n in G, gives us a homomorphism from $G \to S_n$, where G acts transitively on n points. Therefore any subgroup of index 6 in S_6, gives a homomorphism from $S_6 \to S_6$. Pick one of "funny" subgroups of S_6, which is isomorphic to S_5, then we have an automorphism of S_6 which is not inner. If the subgroup is not one of the "funny" ones, it will yield an inner automorphism. □

1.13 Category Theory

1.13.1 Definitions

Definition 1.34. A *category* $\mathbf{C}$ is a collection of objects $\operatorname{Obj}(\mathbf{C})$ such that for any $A, B \in \operatorname{Obj}(\mathbf{C})$, there is a collection $\operatorname{Hom}(A, B)$ of maps (or arrows or morphisms) from A to B. Also, for each $A, B, C \in \operatorname{Obj}(\mathbf{C})$ we have a function

$$\operatorname{Hom}(B, C) \times \operatorname{Hom}(A, B) \to \operatorname{Hom}(A, C) \tag{1.82}$$

where $(g, f) \mapsto g \circ f$ called composition. We also have the following conditions: Furthermore, for each $A \in \operatorname{Obj}(\mathbf{C})$, we have some element $\mathrm{id}_A \in \operatorname{Hom}(A, A)$ called the identity on A such that

1. Associativity: For each $f \in \operatorname{Hom}(A, B)$, $g \in \operatorname{Hom}(B, C)$ and $h \in \operatorname{Hom}(C, D)$ we have $(h \circ g) \circ f = h \circ (g \circ f)$.
2. Identity laws: For all $A, B \in \operatorname{Obj}(\mathbf{C})$, we have $\mathrm{id}_A \in \operatorname{Hom}(A, A)$ and $\mathrm{id}_B \in \operatorname{Hom}(B, B)$ such that for all $f \in \operatorname{Hom}(A, B)$, we have $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$.

Example 1.45. The category **Set** has sets as objects, and the morphisms are set theoretic functions. We also have the category **Grp** where the objects are groups, and the morphisms are homomorphisms. There are analogous categories for many algebraic structures. We also have the category **Top** which consists of topological spaces, where the morphisms are given by continuous maps.

Warning 1.3. At this point professor Borcherds cautioned about investigating mathematical objects that don't have examples of. He suggested one should find some examples before formalizing objects.

Example 1.46. A category with one object is a monoid. If we have inverses this is a group.

Example 1.47. All sets equipped with a partial ordering form a category where the morphisms are given by the inclusion relation.

Definition 1.35. If $\mathbf{C}$ is a category, the dual category is given by simply reversing all of the arrows. This is also written $\mathbf{C}^{\mathrm{op}}$.

1.13.2 Functors

Definition 1.36 (Functor)**.** Given two categories $\mathbf{A}$ and $\mathbf{B}$, a covariant functor between $\mathbf{A}$ and $\mathbf{B}$ is a function:

$$F : \mathrm{Obj}\left(\mathbf{A}\right) \to \mathrm{Obj}\left(\mathbf{B}\right) \tag{1.83}$$

such that for all $A, A' \in \mathrm{Obj}\left(\mathbf{A}\right)$ we have a function

$$F : \mathrm{Hom}\left(A, A'\right) \to \mathrm{Hom}\left(F\left(A\right), F\left(A'\right)\right) \tag{1.84}$$

written $f \mapsto F\left(f\right)$ which satisfies the following axioms:

1. Whenever $A \xrightarrow{f} A' \xrightarrow{g} A''$ we have that $F\left(g \circ f\right) = F\left(g\right) \circ F\left(f\right)$.

2. $F\left(\mathrm{id}_A\right) = \mathrm{id}_{F(A)}$

A contravariant functor G from $\mathbf{A}$ to $\mathbf{B}$ is a covariant functor from $\mathbf{A}^{\mathrm{op}} \to \mathbf{B}$. So a map $A \to A'$ gives rise to a map $G\left(A\right) \leftarrow G\left(A'\right)$. In other words, $G\left(f \circ g\right) = G\left(g\right) \circ G\left(f\right)$.

Example 1.48. The category **Cat** has categories as objects, and functors as the corresponding morphisms.

Remark 1.20. We have foundational issues here. The category **Cat** suggests problems, but considering any category such as **Grp** involves the set of all groups which is an ill defined concept. How do we deal with such things?

1. Only work with objects with elements in some fixed large set

2. Work in a set theory with classes

3. Grothendieck universes

4. Ignore it

we adopt the fourth option.

Example 1.49. We can consider a function $F : \mathbf{Grp} \to \mathbf{Set}$ which sends groups to their underlying sets. This also sends group homomorphisms to the corresponding set theoretic functions. This is called a “forgetful functor” which is a general term used to describe functors which bring sets with structure to their underlying sets.

Example 1.50. This is a motivating example. Consider the homology groups H_i. Then we have a functor

$$\begin{aligned} \mathbf{Top} &\xrightarrow{F} \mathbf{Ab} \\ x &\longmapsto H_i\left(x\right) \end{aligned} \tag{1.85}$$

Example 1.51. The abelianization of a group G, written $G^{\mathbf{Ab}}$, is the smallest normal subgroup of G containing $ghg^{-1}h^{-1}$. Formally we quotient out

$$G/\left\langle \left\{ ghg^{-1}h^{-1} \,|\, g,h \in G \right\} \right\rangle \tag{1.86}$$

Then this gives a functor

$$F : \mathbf{Grp} \to \mathbf{Ab} \tag{1.87}$$

Indeed, if $G \to H$ we get $G^{\mathbf{Ab}} \to H^{\mathbf{Ab}}$

Example 1.52. Consider the categories $\mathbf{Set}, \mathbf{Ab}$. We then have a functor

$$F : \mathbf{Set} \to \mathbf{Ab} \tag{1.88}$$

where a set is mapped to the free abelian group generated by this set. The elements of the free abelian group are:

$$\{n_i s_i \,|\, n_i \in \mathbb{Z}, s_i \in S\} \tag{1.89}$$

where all but a finite number of n_i are 0. If $f : S \to T$ we get $F(f) : F(S) \to F(T)$ which sends $\sum_\alpha n_\alpha s_\alpha \mapsto \sum_\alpha n_\alpha t'_\alpha$

Example 1.53. Let G be a group. Then define a category $\mathbf{G}$ with one object $\{\bullet\} = \mathrm{Obj}(\mathbf{G})$ and $\mathrm{Hom}(\bullet, \bullet) = G$. We notice that the definition of a group satisfies the axioms of a category, with added inverses. Note that if we take a general category with a single object, we only get a monoid.

A functor $F : \mathbf{G} \to \mathbf{Set}$ maps $F(\bullet) = S$ for some set S and for all $g \in G$, $F(g)$ is some function $f : S \to S$. The functor in this case is effectively a set and an action of the group G on this set. In particular, this gives us the permutations of S. The representation of G is a functor from $\mathbf{G}$ to another category.

Example 1.54. Consider the category of vector spaces over some field K. Then we find a functor from this category to itself. The dual of $\mathbf{Vect}_K$ for some field K is a map $F : \mathbf{Vect}_K \to \mathbf{Vect}_K$ such that $F(v) = \mathrm{Hom}(v, k) = v^*$. Now consider $f : v \to w$. Then we want something like $F(f) : F(v) \to F(w)$ but $F(v) : v \to k$ and $F(w) : w \to k$ so this doesn't work.

Instead we see the correct notion is $F(f) : F(w) \to F(v)$. So we get a map $\lambda \to \lambda \circ f$. This is then a contravariant functor since it is in the "wrong" direction.

Example 1.55. Consider the category $\mathbf{Ab}$, and the set $\mathrm{Hom}(A, B)$ for some $A, B \in \mathrm{Obj}(\mathbf{Ab})$. Then a bifunctor in two variables from $\mathbf{Ab} \times \mathbf{Ab} \to \mathbf{Ab}$ is covariant in B and contravariant in A. To see this is covariant in B, we see that if we have $f : B_1 \to B_2$ then from $\mathrm{Hom}(A, B_1)$ we get $\mathrm{Hom}(A, B_2)$ by composition.

To see it is contravariant in A, for $f : A_1 \to A_2$, from $\mathrm{Hom}(A_2, B)$ we get $\mathrm{Hom}(A_1, B)$ by composition. This is the "wrong" way as we saw before. For $g \in \mathrm{Hom}(A_1, B)$, we get the diagram:

$$A_1 \xrightarrow{f} A_2 \xrightarrow{g} B \tag{1.90}$$

1.13.3 Natural Transformations

Example 1.56. Consider a finite dimensional vector space V. We then have the dual vector space V^*, which we know is isomorphic to V itself. This isomorphism is however not-natural, in the sense that one must pick a basis. We do however have a natural isomorphism between V and V^{**} which is simply given by

$$v \mapsto (f : w \mapsto w(v)) \tag{1.91}$$

for $w \in V^*$.

Remark 1.21. As motivated in example example 1.56 we define the concept of a natural isomorphism in terms of functors.

Definition 1.37 (Natural transformation)**.** Consider two categories $\mathbf{C}, \mathbf{D}$ and functors

$$\mathbf{C} \xrightarrow{F} \mathbf{D} \qquad\qquad \mathbf{C} \xrightarrow{G} \mathbf{D} \tag{1.92}$$

then a *natural transformation* is a map $\varphi : F \to G$ such that

$$F(a) \xrightarrow{\varphi(a)} G(a) \tag{1.93}$$

and the following diagram commutes:

$$\begin{tikzcd}
F(a) \arrow[r, "\varphi(a)"] \arrow[d, "F(f)"] & G(a) \arrow[d, "G(f)"] \\
F(b) \arrow[r, "\varphi(b)"] & G(b)
\end{tikzcd} \tag{1.94}$$

Example 1.57. Notice that in the notation of definition 1.37 we have a new category $[\mathbf{C}, \mathbf{D}]$ where $\mathrm{Obj}([\mathbf{C}, \mathbf{D}])$ are the functors from $\mathbf{C} \to \mathbf{D}$ and for two $F, G \in \mathrm{Obj}([\mathbf{C}, \mathbf{D}])$ we have $\mathrm{Hom}(F, G)$ which consists of the natural transformations between these functors.

Example 1.58. Look at $\mathbf{C} = \mathbf{D} = \mathbf{Vect}_k$. Then call the identity F, and the double dual map G.

$$F(v) = v \qquad\qquad G(v) = v^{**} \tag{1.95}$$

Then there exists a natural transformation from F to G. This illustrates the sense that "natural mappings" are natural transformations between functors.

1.13.4 Products, equalizers

Example 1.59. We know products in $\mathbf{Set}, \mathbf{Grp}$ already. These are just the usual Cartesian product:

$$A \times B = \{(a, b) \mid a \in A, b \in B\} \tag{1.96}$$

$$G \times H = \{(g, h) \mid g \in G, h \in H\} \tag{1.97}$$

where the group operation is given by component-wise operation. Topological spaces have the same definition, only the product has the product topology induced by the two initial spaces. But how do we get the same type of object for a general category?

Definition 1.38 (Product)**.** Given a category $\mathbf{C}$, two elements of $A, B \in \mathrm{Obj}\,(\mathbf{C})$ have a product $A \times B$ where $A \times B \in \mathrm{Obj}\,(\mathbf{C})$ and

$$\begin{tikzcd}
& X \arrow[d, dashed, "\varphi"] \arrow[ddl, "f"'] \arrow[ddr, "g"] & \\
& A \times B \arrow[dl, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
A & & B
\end{tikzcd} \tag{1.98}$$

where the morphism from $X \to A \times B$ is unique making the above diagram commutative. This defines $A \times B$ up to canonical isomorphism.

Warning 1.4. We are not guaranteed the existence of products in all categories.

Definition 1.39 (Equalizer)**.** Let $\mathbf{C}$ be a category, and $A, B \in \mathrm{Obj}\,(\mathbf{C})$ with $f, g \in \mathrm{Hom}\,(A, B)$. Then the *equalizer* of A, B is an object $E \in \mathrm{Obj}\,(\mathbf{C})$ and a morphism $i \in \mathrm{Hom}\,(E, A)$ such that $g \circ i = f \circ i$ and for any $C \in \mathrm{Obj}\,(\mathbf{C})$ such that there is some $h \in \mathrm{Hom}\,(C, A)$ where $g \circ h = f \circ h$, then C factors uniquely through E.

$$\begin{tikzcd}
E \arrow[r, "i"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \\
C \arrow[u, dashed] \arrow[ur, "h"] & &
\end{tikzcd} \tag{1.99}$$

Definition 1.40 (Kernel)**.** Suppose A, B groups, $f : A \to B$ is a group homomorphism, and $g : A \to B$ is the trivial homomorphism. Then $\ker(f)$ is the equalizer of

$$\begin{tikzcd}
A \arrow[r, shift left, "g"] \arrow[r, shift right, "f"'] & B
\end{tikzcd} \tag{1.100}$$

Remark 1.22. The motivation here is that we want to define a kernel of a map between two objects without looking inside the objects.

1.13.5 Universality

Definition 1.41 (Initial object)**.** Let $A \in \mathrm{Obj}\,(\mathbf{C})$ for some category $\mathbf{C}$. Then A is an *initial object* iff there exists a unique morphism from A to any other element of $\mathrm{Obj}\,(\mathbf{C})$.

Proposition 1.41. *Initial objects are unique up to isomorphism.*

Example 1.60. The empty set is an initial object in **Set**. The trivial group is an initial object in **Grp**.

Definition 1.42 (Final object)**.** Let $A \in \operatorname{Obj}(\mathbf{C})$ for some category $\mathbf{C}$. Then A is a final object iff there exists a unique morphism from any other element of $\operatorname{Obj}(\mathbf{C})$ to A.

Proposition 1.42. *Final objects are unique up to isomorphism.*

Example 1.61. Any one element set is a final object in **Set**, and the trivial group is a final object in **Grp**.

1.13.6 Limits, Colimits

Definition 1.43 (Limit)**.** Let $\mathbf{C}$ be a category, $\{X_\alpha\}_{\alpha \in I}$ be a family of objects of $\mathbf{C}$, and $\{f_{\alpha_1,\alpha_2}\}_{\alpha_1,\alpha_2 \in I}$ be a family of morphisms where $f_{\alpha_1,\alpha_2} \in \operatorname{Hom}(X_{\alpha_1}, X_{\alpha_2})$. Then the limit of this family of objects is an object $A \in \operatorname{Obj}(\mathbf{C})$ and a collection of morphisms $\pi_\alpha \in \operatorname{Hom}(A, X_\alpha)$ such that

- For any f_{α_1,α_2} we have $\pi_{\alpha_2} = f_{\alpha_1,\alpha_2} \circ \pi_{\alpha_1}$.
- Any other B with these properties factors uniquely through A.

Example 1.62. Consider $A, B, C \in \operatorname{Obj}(\mathbf{C})$ and morphisms $f : A \to B$, $g : B \to C$, $h : C \to A$. Then $X \in \operatorname{Obj}(\mathbf{C})$ equipped with $\pi_1 : X \to A$, $\pi_2 : X \to B$, $\pi_3 : X \to C$ is the limit of A, B, C given that we have the following diagram:

$$\begin{tikzcd}
 & Y \arrow[ddl, bend right, "\varphi_1"'] \arrow[dd, bend right, "\varphi_2"'] \arrow[d, dashed, "\psi"] \arrow[ddr, bend left, "\varphi_3"] & \\
 & X \arrow[dl, "\pi_1"'] \arrow[d, "\pi_2"] \arrow[dr, "\pi_3"] & \\
A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[ll, bend left, "h"]
\end{tikzcd} \tag{1.101}$$

Example 1.63. As it turns out, we have already seen quite a few examples of limits.

- Products: Our objects are A, B with no relevant maps.
- Equalizer: The limit of $A \rightrightarrows B$.

Definition 1.44 (Pullback)**.** Let $A, B, C \in \operatorname{Obj}(\mathbf{C})$ and $f : A \to C$, $g : B \to C$. Then $X \in \operatorname{Obj}(\mathbf{C})$ is called the *pullback* iff it is the limit of A, B, C with morphisms f, g. Note X is equipped with projections to A, B, C and the projection $\pi_1 : X \to A$ is sometimes called the pullback of g by f and $\pi_2 : X \to B$ is sometimes called the pullback of f by g. This is all given by the following diagram:

$$\begin{tikzcd}
Y \arrow[rrd, bend left] \arrow[rdd, bend right] \arrow[rd, dashed] & & \\
& X \arrow[r, "\pi_1"] \arrow[d, "\pi_2"] \arrow[rd, "\pi_3"] & A \arrow[d, "f"] \\
& B \arrow[r, "g"] & C
\end{tikzcd} \tag{1.102}$$

Example 1.64. Let us consider the pullback in **Set**. This means we want a set such that the following diagram commuted.

$$\begin{tikzcd}
X \arrow[r] \arrow[d] & A \arrow[d] \\
B \arrow[r] & C
\end{tikzcd} \tag{1.103}$$

This seems complicated, but it is really somewhat obvious. We just want $X \subset A \times B$ where (a, b) all have the same image in C.

Definition 1.45. The coproduct is the product with all arrows reversed. In other words, the coproduct of $A, B \in \mathrm{Obj}\,(\mathbf{C})$ is some $A \amalg B \in \mathrm{Obj}\,(\mathbf{C})$ such that the following commutes:

$$\begin{tikzcd}
& X & \\
& A \amalg B \arrow[u, dashed, "\psi"] & \\
A \arrow[ruu, "\varphi_1"] \arrow[ru, "p_1"'] & & B \arrow[luu, "\varphi_2"'] \arrow[lu, "p_2"]
\end{tikzcd} \tag{1.104}$$

Example 1.65. The coproduct in **Set** is just the disjoint union (which motivates the above notation $\amalg$). Note for finite products and coproducts these are just the same.

Example 1.66. The finite coproduct in **Ab** is just the product.

Example 1.67. Consider the groups $A = B = \mathbb{Z}$. The coproduct of A, B is the free group on 2 generators. We will see much more on free groups.

Example 1.68. We saw that finite coproducts are just product in **Ab**, but what about infinite products/coproducts?

$$\begin{tikzcd}
& A_1 \times A_2 \times \dots \arrow[ld] \arrow[d] \arrow[rd] & \\
A_1 \arrow[rd] & A_2 \arrow[d] & A_3 \dots \arrow[ld] \\
& \text{subset of } A_1 \times \dots &
\end{tikzcd} \tag{1.105}$$

The infinite product in **Ab** is just the usual product. The infinite coproduct is then the subset of the infinite product such that all but finitely many of the coordinates vanish. This is because if the coproduct were simply the product it would not be universal.

1.14 Free groups

1.14.1 Free abelian groups

Definition 1.46. The *free abelian group* on n generators $\{g_i\}_{i=1}^n$ is the group of elements of the form

$$\sum_{i=1}^{n} n_i g_i \tag{1.106}$$

where $n_i \in \mathbb{Z}$ for all i.

Proposition 1.43. *There is a unique isomorphism $\mathbb{Z}^n \cong G$ for any free abelian group G. Explicitly this brings $e_i \to g_i$. Putting this in categorical terms, we have that the free abelian group is the coproduct of n copies of $\mathbb{Z}$.*

$$\begin{tikzcd}
\mathbb{Z} \arrow[drr] \arrow[ddrr] & \mathbb{Z} \arrow[dr] \arrow[ddr] & \cdots & \mathbb{Z} \arrow[dl] \arrow[ddl] & \mathbb{Z} \arrow[dll] \arrow[ddll] \\
& & \mathbb{Z}^n \arrow[d, dashed] & & \\
& & X & &
\end{tikzcd} \tag{1.107}$$

Remark 1.23. Recall that the finite coproduct and product are the same in an Abelian group.

Definition 1.47. Let $G \cong \mathbb{Z}^n$ be a free abelian group. Then the exponent n is the rank of G.

Remark 1.24. It is worth considering if this notion of rank is even well defined. It turns out to be since the number of homomorphisms mapping $\mathbb{Z}^n$ to $\mathbb{Z}/2\mathbb{Z}$ is 2^n.

Proposition 1.44. *Any subgroup of $\mathbb{Z}^n$ is free of rank $\leq n$.*

Proof. Recall the proof that finite abelian groups are the same as products of cyclic groups. We showed that for $A \subseteq \mathbb{Z}^n$ we can find generators $g_1, \cdots, g_n$ of $\mathbb{Z}^n$ meaning A is generated by

$$n_1 g_1, n_2 g_2, \cdots \tag{1.108}$$

for some $\{n_i\}$. Therefore A is free of rank $\leq n$. □

1.14.2 Free groups

Definition 1.48. The free group on generators $\{g_i\}_0^n$ is the universal group generated by these elements.

Remark 1.25. This means it maps uniquely to any other group generated by $G_1, \cdots, G_n$ by $g_i \to G_i$. Again this is the coproduct of $\mathbb{Z}, \cdots, \mathbb{Z}$ only now in **Grp** rather than **Ab**.

Remark 1.26. The free group should be thought of as consisting of words consisting of the generators. Then the binary relation is just concatenation, which is clearly associative. We clearly want the notion of aa^{-1} to be the identity, or the empty word, so there is some work to be done to see that this construction gives us the free group explicitly.

Example 1.69. Suppose we have the generators $\{a, b, c\}$. Take all words in the symbols:

$$\left\{a, a^{-1}, b, b^{-1}, c, c^{-1}\right\} \tag{1.109}$$

which includes the empty string. Then these have associative product $x \times y = xy$ where the identity is the empty string. As of now this is just a free monoid on three elements. So what about inverses?

Now we just need to force these to be inverses of one another. Force a^{-1} to be the inverse of a. Now we take the smallest equivalence relation such that

1. $a^{-1}a \equiv 1, a^{-1}a \equiv 1$
2. If $a \equiv b$ then $ac \equiv bc$, so $ca \equiv cb$ which makes the product well defined on equivalence classes.

So we take all words on the set of all elements generated by these three generators modulo this equivalence relation. This gives us the Free group on three elements.

Example 1.70. Now what does the actual free group look like? The construction above leads us to believe the elements can be identified with reduced words. This just means we don't allow adjacent "inverses" in words. So if A, B are two different reduced words, do they correspond to different elements of the free group? Yes. Look at ab^{-1}. If A is a reduced word other than 1, show that A is not 1.

So if we have

$$aba^{-1}b^{-1}cbab^{-1}a^{-1}c^{-1} \tag{1.110}$$

do we know that this is not-equivalent to the empty string? This is very difficult, so instead we prove something somewhat stronger.

Theorem 1.15. *If A is reduced and not the empty string, we can find finite group G and map from the free group to G such that the image of A is not* 1.

Remark 1.27. This is the statement that free groups are residually finite. This means non-trivial elements can be detected by finite groups.

Proof. Let $G = S_n$ for $n = 1+$ the length of the word A. We illustrate the argument with a specific example. Let $A = b^{-1}a^{-1}ba^{-1}ba$. Then we have the following graph:

$$\circ \xrightarrow{a} \circ \xrightarrow{b} \circ \xrightarrow{a^{-1}} \circ \xrightarrow{b} \circ \xrightarrow{a^{-1}} \circ \xrightarrow{b^{-1}} \circ$$

Note there are $7 = 1+$length of the word points in the above diagram. Now we desire to complete this to some permutation of S_7.

This is not possible if we have two adjacent jumps which either hit head-on, or go opposite directions. But we notice that this would only be the case if we didn't have a reduced word, since

$$\begin{array}{ccc} \circ \xrightarrow{a} \circ \xleftarrow[a]{} \circ & \iff & \circ \xrightarrow{a} \circ \xrightarrow{a^{-1}} \circ \\ \\ \circ \xleftarrow[a]{} \circ \xrightarrow{a} \circ & \iff & \circ \xrightarrow{a^{-1}} \circ \xrightarrow{a} \circ \end{array} \tag{1.111}$$

Now we map a to a permutation σ_a such that $\sigma_a(1) = 2$, $\sigma_a^{-1}(3) = 4$, and $\sigma_a^{-1}(5) = 6$, and we must send b to a permutation σ_b with $\sigma_b(2) = 3$, $\sigma_b(4) = 5$, and $\sigma_b^{-1}(6) = 7$. The constraints on a^{-1} become constraints on a by noting that $\sigma_a^{-1}(x) = y$ iff $\sigma_a(y) = x$. The same holds for b^{-1}. Then A gets mapped to the permutation $\sigma_b^{-1}\sigma_a^{-1}\sigma_b\sigma_a^{-1}\sigma_b\sigma_a$, and this permutation sends the leftmost vertex, representing element 1, to the rightmost vertex, representing the element $n = 7$. □

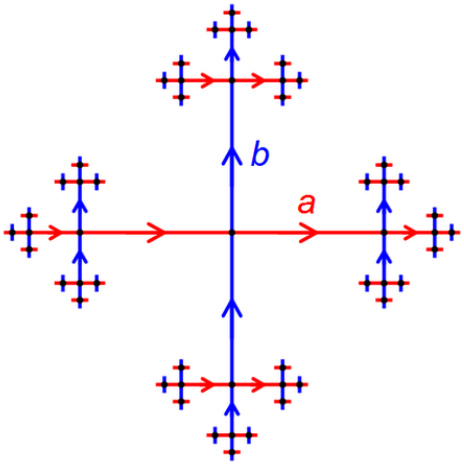
Example 1.71. Let's look at some visual representations of these groups. A free abelian group on two elements will look like a big grid, with a mapping in one direction and b in the other direction.

The non-abelian case exhibits hyperbolic geometry, and is "exponential". An explicit isometry is given by:

$$\tau \mapsto \frac{a\tau + b}{a\tau + d} \tag{1.112}$$

where

$$\mathrm{SL}_2(\mathbb{Z}) \ni \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 2 \tag{1.113}$$

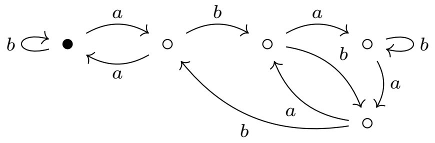


1.14.3 Subgroups of free groups

Warning 1.5. Subgroups of free groups are free, but may have larger rank.

Example 1.72. Look at the cosets of $G \subseteq F$, and let F act on the set of left cosets. This gives the action of the generators of the group on the cosets. Pick some point as the base point. Then the number of subgroups of index n of F are in bijection with the connected graphs on n points, with G-colored cycles.

Example 1.73. Consider some index 5 subgroup.



(1.114)

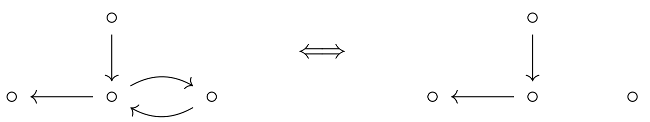
Now if we pick a base point, we get a subgroup of index 5.

Definition 1.49. Here, homotopy classes mean that two paths are equivalent if the difference between the two are just edges traversed that were immediately retraced backwards.

Remark 1.28. The idea of a homotopy class is retracting double crossed edges and not "changing" the path.

Definition 1.50. The fundamental group of a graph consists of the homotopy classes of loops from the base point back to itself where loops follow the edges of the graph.

Example 1.74. Suppose G is a subgroup of a free group F. Then we look at the graph of G (cosets F/G). So G is just loops from the base point back to itself. In other words, it is the fundamental group of the graph.



(1.115)

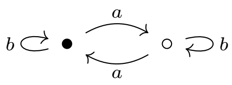
This is what gives us inverses as well because travelling one way down the path is the inverse of travelling the other way.

Example 1.75. The fundamental group of a graph mapping from a single node back to itself three times is the free group on 3 generators.

Proposition 1.45. *The fundamental group of a graph consisting of a single vertex mapping back to itself n times is the free group on n generators. Conversely, the fundamental group of any graph is free.*

Proof. The idea here is that we can pick an edge with distinct vertices and contract edges. This doesn't change the fundamental group of the graph. So keep contracting edges until it is a single node, and the fundamental group is a free group on the number of loops. □

Example 1.76. Consider the free group F_2 on (a, b). And $G \subseteq F_2$ a subgroup of index 2.



(1.116)

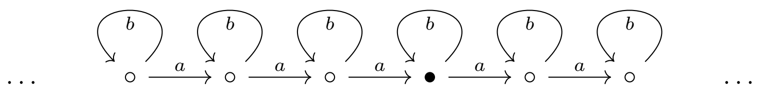
Now contracting the middle we get a free group on three elements:

$$b, a^2, a^{-1}ba \tag{1.117}$$

this is a subgroup of the free group on 2 generators.

Remark 1.29. In general, to get the generators, go along tree to start of edge, do edge, then back along the tree.

Example 1.77. Is every subgroup of a finitely generated free group finite? We consider a subgroup of F_2 that is not finitely generated:



(1.118)

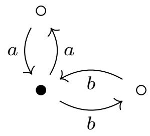
is a subgroup of F_2. All words lead back to the base point, so the fundamental group of graph is the free group with

$$\left\{a^n b a^{-n} : n \in \mathbb{Z}\right\} \tag{1.119}$$

as generators.

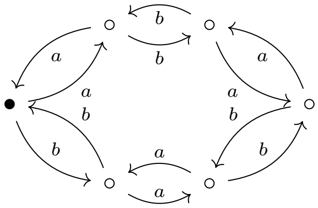
Remark 1.30. What about countability? Professor Borcherds says: if you are doing algebra with objects of uncountable cardinality you are some sort of set theorist pretending to do algebra.

Example 1.78. Map $F_2 \to S_3$ where we have that $a^2 = b^2 = 1$ and $(ab)^3 = 1$. Then we have



(1.120)

Is ker of the map from $F_2 \to S_3$ free? Well, we know it is the the smallest normal subgroup containing $a^2, b^2, (ab)^3$. This is greater than the smallest subgroup. In particular it is a subgroup of index 6.



Note this diagram is so symmetric because the subgroup is normal. We can contract the interior edges to get 7 generators for the kernel.

Proposition 1.46. *If G has index n in F_m then G has $n(1-m)$ generators.*

Proof. First note that the graph of F_m has Euler characteristic $1-m$. The graph of G has n vertices, mn edges, so the Euler characteristic is $n - mn = (1-m)n$ so the number of generators is $n(1-m)$ □

Chapter 2

Rings

2.1 Definitions and examples

Definition 2.1 (Ring)**.** A *ring* is a set R along with two binary operations, $+$ and $\times$, such that:

1. R is an abelian group under $+$
2. $\times$ is associative
3. $a\left(b+c\right)=ab+ac$, $\left(a+b\right)c=ac+bc$

We also have two optional axioms:

1. $\times$ has an identity
2. $ab=ba$ (commutative rings).

Remark 2.1. One often consider rings without an identity element in analysis.

Remark 2.2. In some literature there is a much more complicated notion of rings. For example, it is easy to see simple examples of the following:

1. **Rg**: Set X with two binary operations $+, \cdot$ such that $+$ gives the structure of a commutative monoid, $\cdot$ gives a semigroup, and $\cdot$ distributed over $+$.
2. **Rig**: A **Rg** with multiplicative identity.
3. **Rng**: A **Rg** with additive inverses. This is our definition of ring from above.
4. **Ring**: A **Rig** with additive inverses (or equivalently a **Rng** with a multiplicative identity.) This is our definition of a ring with our first optional axiom.
5. **Cring**: A commutative **Ring**. This is our definition of ring with both optional axioms.

We will see more methods of classifying rings such as integral rings and division rings.

Definition 2.2 (Unit)**.** Let R be a ring. An element $a \in R$ is a *unit* iff it has a multiplicative inverse in R. We denote the collection of all invertible elements of R as $R^{\times}$.[2.1]

Proposition 2.1. *Let R be a ring. The group of units, $R^{\times}$ is a group. If we let R be a cring, $R^{\times}$ becomes an abelian group.*

Example 2.1. The integers $\mathbb{Z}$ are a ring.

Example 2.2. The Gaussian integers,

$$\mathbb{Z}[i] = \left\{ m + ni : m, n \in \mathbb{Z}, i^2 = -1 \right\} \tag{2.1}$$

are a ring.

Example 2.3. Polynomials in a variable x over a field K, $K[x]$, are a ring.

Example 2.4. The set of $n \times n$ matrices with entries in K, $M_n(K)$, is a ring.

Example 2.5. The Burnside ring of a group $G = S_3$ is the set of all sums $\sum n_i A_i$ for $n_i \in \mathbb{Z}$ and A_i some transitive permutation representation of G (up to isomorphism). The 4 transitive permutation representations of S_3 are conjugacy classes:

$$\left\{1, (1\,2)\right\}, \left\{1, (1\,3)\right\}, \left\{1, (2\,3)\right\}, \left\{1, (1\,2\,3), (1\,3\,2)\right\} \tag{2.2}$$

We get the adjoint representation of 6 points, 3 points, 2 points, and 1 point, so we get sums of the form:

$$aA^1 + bA^2 + cA^3 + dA^6 \tag{2.3}$$

Any permutation representation is the union of transitive ones. So the set of all finite permutation representations (up to isomorphism) is the elements of the form $aA^1 + bA^2 + cA^3 + dA^6$. This is not a ring, but we can force it to be one by adding subtraction. This is the same thing one does in the construction of the integers from the natural numbers. Doing this to any commutative monoid returns what is called the Grothendieck group.

The addition + in this ring is the disjoint union of representations. × in this ring is the product of permutation representations. In particular, we have the multiplication table:

$\times$	A^1	A^2	A^3	A^6
A^1	A^1	A^2	A^3	A^6
A^2	A^2	$A^2 \oplus A^2$	A^6	$A^6 \oplus A^6$
A^3	A^3	A^6	$A^3 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$
A^6	A^6	$A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6$

[2.1] This is also denoted by R^* but we choose this alternative notation with an eye towards duality of modules.

2.2 Group rings

- A set S (in relation to groups) can be understood to correspond to the vector space with basis S (in relation to rings).
- The symmetric group S_n corresponds to $M_n(K)$ (linear transformations of K^n)[2.2]
- We study a group G by making G act on some set. We study rings by making them act on K^n.
- Sets A, B have $A \amalg B$ and $A \times B$ with elements of the form $a + b$ and ab, respectively. Given vector spaces V, W with respective dimensions a and b, $V \oplus W$ has dimension $a + b$, and the tensor product[2.3] $V \otimes W$ has the property that if A is a basis for V and B is a basis for W, then $A \times B$ is a basis for $V \otimes W$, so $V \otimes W$ has dimension ab.
- We know that
$$|A \cup B| = |A| + |B| - |A \cap B| \tag{2.4}$$
Similarly, if V and W are vector spaces,
$$\dim(V \cup W) = \dim(V) + \dim(W) - \dim(V \cap W). \tag{2.5}$$

Warning 2.1. For sets $D = A \cup B \cup C$, then $|D| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$ This is not true for vector spaces. Let U, V, W be 2 dimensional vector space in $\mathbb{R}^3$ containing some fixed line.

Definition 2.3. Let G be a group and R a commutative ring. The *group ring* $R[G]$ is the free abelian group with basis G, where $\times$ is the group operation on G extended linearly.

Example 2.6. Let G be the Klein 4 group $\{1, a, b, c\}$ with
$$a^2 = b^2 = c^2 = 1, ab = c, \cdots \tag{2.6}$$
So $\mathbb{C}[G]$ is a four dimensional vector space with basis a, b, c, d. It is a product of 4 copies of the ring $\mathbb{C}$. Look at
$$e_1 = (1 + a + b + c)/4 \qquad e_2 = (1 + a - b - c)/4 \tag{2.7}$$
$$e_3 = (1 - a + b - c)/4 \qquad e_4 = (1 - a - b + c)/4 \tag{2.8}$$
Note that $e_i e_j = 0$ (if $i \neq j$) and $e_i^2 = e_i$. This latter statement says that the e_i are *idempotent*.

[2.2] S_n is the Weyl group of $\mathrm{GL}_n(K)$

[2.3] In older texts, this is sometimes referred to as the Kronecker product

Proposition 2.2. *More generally, for a ring R, suppose $e \in R$ is idempotent. Then we have:*

$$R = eR \oplus (1-e)\,R \tag{2.9}$$

both of which are rings. Conversely, in $A \times B$, $(1,0)$ is idempotent. So the presence of idempotents is equivalent to the ring splitting as a product.

Example 2.7. Let G be the monoid $G = \mathbb{N}$. Then $\mathbb{Z}\,[G]$ is still a ring if we take our basis to be $x^0, x^1, \cdots$. This makes

$$\mathbb{Z}\,[G] = \left\{n_0x^0 + n_1x^1 + \cdots \mid n_0, n_1, \cdots \in \mathbb{Z}\right\} \tag{2.10}$$

the polynomial ring. If we take $G = \mathbb{Z}$, we get the Laurent polynomials in $\mathbb{Z}$.

Definition 2.4. We can think of elements of $R\,[G]$ as functions from $G \to R$, where $f\,(g_i) = r_i$. Then the product of $R\,[G]$ is given by

$$fh\,(g) = \sum_{g_1g_2=g} f\,(g_1)\,h\,(g_2) \tag{2.11}$$

which is called the *convolution* of f and h.

Example 2.8. Let $G = \mathbb{R}$, which is not finite. Consider the ring of all compactly supported continuous functions f. Then

$$f * h\,(x) = \int f\,(y)\,h\,(x-y)\,dy \tag{2.12}$$

is another type of convolution. This is a ring under convolution, but it does not have an identity element for convolution.[2.4]

2.3 Ideals

Remark 2.3. Ideals correspond to normal subgroups which we recall were kernels of homomorphisms. We define ideals by the properties we need for the kernel of a homomorphism.

Definition 2.5. An ideal I of a ring R is a subset of R such that:

1. I contains 0_R and is closed under addition and subtraction (I is a normal subgroup of R with respect to addition.)

2. If $r \in I$, and $t \in R$ then $rt, tr \in I$ (stronger than saying that I is closed under ×.)

Remark 2.4. We must check that the two conditions above are sufficient. Suppose I satisfies these. Can we form R/I? Addition is well defined since I is a normal subgroup of R with respect to addition. To see if multiplication is well

[2.4] The Dirac δ distribution is actually an identity for convolution for a larger ring than this.

defined, we first define multiplication to be $(aI)(bI) = (ab)I$. We want to see if $a \equiv b$ and $c \equiv d$ (or equivalently if $a - b \in I$ $c - d \in I$) imply that $ac \equiv bd$, or $ac - bd \in I$. Let $b = a + i_1$ and $d = c + i_2$. Then

$$\begin{aligned} ac - bd &= ac - (a + i_1)(c + i_2) && (2.13)\\ &= ac - ac - i_1 c - i_2 a - i_1 i_2 && (2.14)\\ &= -i_1 c - i_2 a - i_1 i_2 && (2.15) \end{aligned}$$

and all three terms in the last line are in I. If S is any subset of a ring R, we can force S to be 0 by taking the smallest ideal $I \supseteq S$. In this case, I is the set of finite sums of the form $\sum_{s_i \in S} r_i s_i t_i$ with $r_1, t_i \in R$.

2.4 Generators and relations

Example 2.9. If we want to form a ring out of a set S, we have 2 choices:

1. Free commutative ring: First form the free commutative monoid on S. If $S = \{x, y, z\}$, then this is $\{x^{n_1} y^{n_2} z^{n_3} : n_1 \in \mathbb{N}\}$ The free commutative ring is the ring
$$\left\{n_{a,b,c} x^a y^b z^c : a, b, c \geq 0\right\} \qquad (2.16)$$
Say we have the elliptic curve $y^2 = x^3 - x$. We can form the coordinate ring $\mathbb{Z}[x, y] / \left(y^2 - x^3 + x\right)$ where we are quotienting out by the ideal generated by $y^2 - x^3 + x$.

2. Noncommutative free ring: Take the noncommutative free monoid on $\{x, y, z\}$. This is all words in $\{x, y, z\}$. The noncommutative free ring is the group ring of the free monoid.

   Now we can construct rings such as $\mathbb{Z}[x, y, z] / \left(x^2 + y^2 z - z y^2\right)$ (some ideal generated by some elements), which is noncommutative.

Example 2.10. Suppose A and B are rings. We can construct the coproduct as follows: assume $A \cap B = \emptyset$, and form the free ring F on the set $A \cup B$. Quotient out by an ideal to force the map from $a \to F$ to be a homomorphism; we have

$$I = (f(a + b) - f(a) - f(b), f(ab) - f(a) f(b)) \qquad \forall a, b \in R \qquad (2.17)$$

and so on (including all the relations we want). Then F/I is the coproduct of A and B.

Example 2.11. The coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in the category of rings is the free non-commutative ring on x, y. However, the coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in the category of commutative rings is the polynomial ring $\mathbb{Z}[x, y]$.

2.5 Integral domains

Definition 2.6 (Integral domain)**.** A ring R is an integral domain iff $1 \neq 0$, it is commutative, and there are no zero divisors in the ring.

2.5.1 Euclidean domains

Example 2.12. Recall that every integer $\neq 0$ is a product of primes in an essentially unique way. $12 = 2 \times 2 \times 3 = (-2) \times (-2) \times 3$ which is unique up to order and multiplication by units.

This was effectively shown by Euclid. The key point he used was division with remainder. That is, given a, b with $a \neq 0$, we can write $a = bq + r$ where $r < b$.

What order do we have in this context? For integers, this means $|r| < |b|$. We can do the same thing for polynomials $a, b \in \mathbb{R}[x]$. In this case, smaller means that the degree is smaller (or $a = 0$).

Definition 2.7 (Euclidean Domain)**.** A cring R is a *Euclidean domain* iff it has a function $|\cdot| : R \to \mathbb{N}$ such that given a, b with $b \neq 0$, we can find r, q such that $a = bq + r$ and $|r| < |b|$.[2.5]

Example 2.13. Consider the Gaussian integers:

$$Z[i] = \left\{a + bi : a, b \in \mathbb{Z}, i^2 = -1\right\} \tag{2.18}$$

Now we define $|a + bi| = a^2+b^2$. This is the usual Euclidean norm but squared to make sure we get an integer. Given a, b we need to find r, q such that $a = bq+r$, which means $a/b = q+r/b$, where $|r/b| < 1$. Given any a/b, we can find $q \in Z[i]$ of distance < 1 from a/b. Draw an open disk of radius 1 around each element of $Z[i]$. These cover $\mathbb{C}$, so we can find r, q.

2.5.2 Principle Ideal Domains

Definition 2.8. The *ideal generated by* elements $g_1, g_2, \cdots$ is the smallest ideal containing these elements. We write this as $(g_1, g_2, \cdots)$.

Definition 2.9. A *principal ideal domain* is a commutative ring where all ideals are generated by one element.

Example 2.14. $\mathbb{Z}$ is a principal ideal domain. In $\mathbb{Z}$ we only have ideals of the form $n\mathbb{Z}$.

Example 2.15. Here is an example of a commutative ring that is not a PID. Let $R = \mathbb{C}[x, y]$, and let $I = (x, y)$ be the set of all polynomials with constant term 0. If $I = (f)$, then f divides x and f divides y. This means $f = 1$, but $1 \notin (x, y)$.[2.6]

Theorem 2.1. *All euclidean domains are PIDs.*

[2.5] We don't actually need the codomain of the norm function to be $\mathbb{N}$. We just need it to be well-ordered. In practice, however, the useful examples are all concerning $\mathbb{N}$, so this isn't a particularly useful generalization.

[2.6] The entire field of algebraic geometry apparently rests on the idea that not all of these ideals are principal.

Proof. Let I be any ideal. We then choose $a \in I$ with $a \neq 0$, and $|a|$ minimal. Then we claim that $I = (a)$.

Suppose $b \in I$. Then $b = aq + r$ with $|r| < |a|$. So $r = b - aq$ means that $r \in I$, and the minimality of $|a|$ forces $r = 0$. This means $b = aq$ for some q, and this holds for any $b \in I$, for $I = (a)$. □

Example 2.16. We consider $R = \mathbb{Z}\left[(1 + \sqrt{-19}/2\right]$. This is a PID which is not euclidean. In other words a counterexample to theorem theorem 2.1. To see that R is a PID, see an algebraic number theory course.[2.7]

Here is a sketch that R is not euclidean. Let $a \in R$ such that a is not zero, and is not a unit. So every element of $R/(a)$ is represented by 0 or a unit. The only units of R are ± 1, so $R/(a)$ has ≤ 3 elements. If $a \neq \pm 1, 0$ then $R/(a)$ has ≥ 4 elements (in fact $|a|^2$ elements).

2.5.3 Unique factorization domains

Definition 2.10 (Divides)**.** Let $a, b \in R$. We say *a divides b* and write $a|b$ iff there exists some $c \in R$ such that $ac = b$.

Definition 2.11 (Irreducible)**.** An element $a \in R$ is called *irreducible* in R iff it is not 0, it is not a unit, and $a = bc$ implies either b or c is a unit.

Definition 2.12 (Prime)**.** An element $a \in R$ is called *prime* iff $a|bc$ implies that $a|b$ or $a|c$.

Remark 2.5. For $\mathbb{Z}$ prime elements are exactly irreducible elements, but this is not the case for most rings. Let's look a bit closer at how these two concepts relate to one another in a general ring.

Lemma 2.1. *In a principal ideal domain, irreducible elements are also prime.*

Proof. Suppose p is irreducible and $p|ab$. We want to show that either $p|a$ or $p|b$. Suppose that $p \not| a$. Then we must have some element of $c \in R$ such that the ideal (p, a) is the same as (c) since R is a principal ideal domain by assumption.

Now we have that $c|p$ but since p is irreducible, c must be either a unit, or p up to a unit. If c is a unit multiple of p, then since we have that $c|a$, we must have $p|a$ which is a contradiction. So this means c is a unit. We now know that the ideal generated by c must contain 1, and therefore $(c) = R$.

It follows from this that there are elements $x, y \in R$ such that $px + ay = 1$. So $pbx + aby = b$ and since both of the terms on the LHS are divisible by p, we have that $p|b$ and p is prime as desired. □

Proposition 2.3. *If R is an integral domain, prime elements are irreducible.*

Proof. Consider some prime p. If $p = ab$, then $p|ab$, so WLOG assume $p|a$. Then $a = pc$ for some $c \in R \setminus 0$ which means $pc = a = abc$ and $a(1 - bc) = 0$ so $bc = 1$, and b is a unit, making p irreducible. □

[2.7] See for example Lang [`?lang_alg_num`].

Definition 2.13. A commutative ring R is a *unique factorization domain* iff every element in R can be expressed uniquely as a product of irreducible elements, up to order and unit multiples.

Proposition 2.4. *If R is a UFD, then every irreducible element is prime.*

Proof. Assume $q \in R$ is irreducible. Then if $q|ab$ for $a, b \in R$, we have that for some $m \in R$, $mab = q$. Since this is a UFD, we have some unique representation of m, a, b up to units. Therefore, up to units, for irreducible elements $m_1, \cdots, m_i, a_1, \cdots, a_j, b_1, \cdots, b_k \in R$, we have that

$$q = m_1 \cdots m_i a_1 \cdots a_j b_1 \cdots b_k \tag{2.19}$$

but now taking any split of this product, one factor must be a unit, since q is irreducible. This means we can split appropriately, to find that either $q|a$ or $q|b$ as desired. □

Theorem 2.2. *Every principal ideal domain is a unique factorization domain.*

Proof. Let R be a PID. We first show existence of a factorization of any element into irreducibles. Given any element $a \in R$, if a is not a unit, we can find some irreducible $p \in R$ such that $p|a$. Let $a = bc$ for some $bc \in R$. If b is irreducible we stop, if not we write $b = de$ for some $de \in R$. Now repeat this process until it stops. Will this go on forever?

No. Suppose we have an ideal generated by $a_1, a_2, \cdots$ where $a_1 = a_2' a_2, a_2 = a_3' a_3, \cdots$ with $a_1', a_2', \cdots$ not units. We know that there is some x such that (a) is equal to $(a_1, a_2, \cdots)$ since this is a principal ideal domain. Therefore $x \in (a, a_1, \cdots, a_n)$ for some finite enumeration of elements of $a_1, a_2, \cdots$ so the sequence must stop after finitely many steps.

Now take $a = bc$ with b irreducible, $c = de$ with d irreducible and so on, for finitely many steps. So every non-zero element is a product of irreducibles.

Remark 2.6. Note this is actually true in a more general case. This only relies on the fact that a ring is *Noetherian.* That is, that there are no strictly increasing sequences of ideals $I_1 \subset I_2 \subset I_3 \cdots$.

We now show that this representation is unique. This is the first step in the proof to require an original idea. The key step here is that we recall and use that irreducibles are prime. Suppose we have two representations:

$$a = p_1 \cdots p_m = q_1 \cdots q_n \tag{2.20}$$

with all p_i, q_i irreducible. We want to show that these factorizations are unique up to order and multiplication by units. Since we know p_1 is irreducible, p_1 is prime, and therefore p_1 divides some q_i. But q_i is irreducible, so q_i must then just be a unit multiple of p_1. We can "cancel" from both sides. Formally, this is equating the difference of the two representations, factoring out p_1, and asserting that the rest is 0. Repeating this gives us our desired results. □

Example 2.17. Let R be the set of polynomials of positive rational power. An example of this is:

$$3 + 3x^{5/7} + 2x^{17/3} \tag{2.21}$$

This argument goes wrong here because $x = x^{1/2}x^{1/2}$

$$x = x^{1/2}x^{1/2} = x^{1/4}x^{1/4}x^{1/4}x^{1/4} = \cdots \tag{2.22}$$

which goes on forever. In other words, the ideal $\left(x^{1/2}, x^{1/4}, \cdots\right)$ is not principal.

Example 2.18. Suppose $a + bi \in \mathbb{Z}[i]$ is prime. Then $(a+bi)(a-bi) = a^2 + b^2 \in \mathbb{Z}$. We can then use this method to factor elements in $\mathbb{Z}$ to become elements in $\mathbb{Z}[i]$. For example $5 = 2^2 + 1 = (2+i)(2-i)$.

$$65 = 5 \times 13 = (2+i)(2-i)(3+2i)(3-2i) = (4+7i)(4-7i) = (8-i)(8+i) \tag{2.23}$$

because we have $65 = 4^2 + 7^2 = 8^2 + 1^2$ we get a correspondence between the ways to factor some $x \in \mathbb{Z}$ in the $\mathbb{Z}[i]$ and the ways to write x as a sum of squares.

Example 2.19. Consider the ring $R = \mathbb{Z}\left[\sqrt{-2}\right]$. Now imagine this as a rectangular lattice in $\mathbb{C}$. The circles of radius 1 around these points cover $\mathbb{C}$, so as we argued before with $\mathbb{Z}[i]$, we have that $\mathbb{Z}\left[\sqrt{-1}\right]$ is a euclidean domain, and therefore also a unique factorization domain.

If we instead consider $R = \mathbb{Z}\left[\sqrt{-3}\right]$ we notice that circles of radius 1 with centers at each element of this ring do not cover $\mathbb{C}$ anymore, since these are open disks and we have the point $\left(1/2, \sqrt{-3}/2\right)$ which is not covered. This is related to the fact that R is not a unique factorization domain. We have:

$$2 \times 2 = \left(1 + \sqrt{3}i\right)\left(1 - \sqrt{3}i\right) \tag{2.24}$$

and ± 1 are the only units in R. These are all irreducible elements. If $2 = ab$, then $|a|\,|b| = |2| = 2$, which means $|a| = \pm 1$ or $|b| = \pm 1$.

Remark 2.7. Multiplying $z \in R$ by a scales $|z|$ by $|a|$ and essentially rotates by $\arg(a)$. So a principal ideal in $\mathbb{Z}\left[\sqrt{-3}\right]$ looks like a rotated and rescaled rectangular lattice. But what does a non-principal ideal look like? Look at $\left(2, 1 + \sqrt{-3}\right)$ which gives a diamond lattice instead of a rectangular one.

Remark 2.8. Note that unique factorization domains do not need to be principal ideal domains. We illustrate this with some counterexamples.

Example 2.20. The ring $\mathbb{Z}[x]$ is a unique factorization domain, yet it also has the non-principal ideal $(2, x)$.

Example 2.21. Let K be a field. $K[x, y]$ is a unique factorization domain and has the non-principal ideal (x, y).

Remark 2.9. We will eventually see that if R is a unique factorization domain, this gives us that $R[x]$ (the polynomials over R) is also a unique factorization domain.

Theorem 2.3 (Fermat). *Any prime $p \in \mathbb{Z}$ where $p > 0$ and $p \equiv 1 \pmod 4$ can be uniquely expressed as $a^2 + b^2$ up to sign changes for a, b.*

Proof. We know $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1 = 4n$ for some $n \in \mathbb{Z}$. We also know it has $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ which has order 2. If we have that $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is the generator, then by definition we have that $g^{4n} = 1$ which means

$$-1 \equiv g^{2n} \pmod p \tag{2.25}$$

so -1 is a square modulo p. This means that for some $n, a \in \mathbb{Z}$ it is the case that:

$$-1 = a^2 - np \tag{2.26}$$

Therefore, $np = a^2 + 1 = (a + i)(a - i)$ in $\mathbb{Z}[i]$. In particular,

$$p|\,(a + i)(a - i) \tag{2.27}$$

but does not divide either of $(a \pm i)$ Therefore p is not prime and therefore not irreducible in $\mathbb{Z}[i]$. This means for some $a, b \in \mathbb{Z}$ we have $p = (a + bi)(a - bi)$ where we know the decomposition must be of this form, since any other form would not yield a real product. Therefore, $p^2 = a^2 + b^2$.

To see uniqueness, we assume that we have $p = x^2 + y^2$. Then we know $p = (x + iy)(x - iy)$ so we have that $z + iy = u(a + bi)$ where u is some unit of $\mathbb{Z}[i]$ since we know it is a unique factorization domain. This all means $x = \pm 1$ and $b = \pm b$ as desired. □

2.6 Ideals of commutative rings

Definition 2.14 (Integral domain). A cring R is an *integral domain* iff for $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

Definition 2.15 (Field). A cring is a field iff it has no zero divisors, and every element has a multiplicative inverse.

Definition 2.16 (Maximal Ideal). An ideal I of a ring R is a *maximal ideal* iff it is the maximal element of the proper ideals of R.

Definition 2.17 (Prime ideal). An ideal I of a ring R is a *prime ideal* iff

$$ab \in I \implies a \in I \wedge b \in I \tag{2.28}$$

Theorem 2.4. *An ideal I of a ring R is maximal iff R/I is a field.*

Theorem 2.5. *An ideal I of a ring R is prime iff R/I is an integral domain.*

Theorem 2.6. *Maximal Ideals are always prime ideals (but not the other way around)*

Theorem 2.7. *The maximal ideal of a field is always 0.*

Proof. Assume F is a field. This means 0 is the maximal ideal. Now assume 0 is the maximal ideal of some ring R. Then it is the case that $R = (a)$ for some nonzero a. So $ab = 1$ for some $b \in R$ which means a has an inverse. □

Remark 2.10. These are the two most important classes of ideals of rings.

Example 2.22. If we consider the ring $\mathbb{Z}$, the ideals are all of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$. The maximal ideals are $n = p$ for prime p. The prime ideals are the maximal ideals and the ideal (0).

Example 2.23. Consider the ring $\mathbb{C}[x]$. Ideals of this ring are of the form (f) for some polynomial f. Therefore the maximal ideals are $(x - a)$ for some $a \in \mathbb{C}$. This is because for all polynomials of degreee greater than 1, we can find a factorization as $f = gh$ for some g, h so $(f) \subseteq (g)$ but that would mean it wasn't maximal. The prime ideals are the maximal ideals plus the ideal (0).

Example 2.24. We now consider the complex polynomials in two variables: $\mathbb{C}[x, y]$. The maximal ideals of this ring are of the form $(y - a, y - b)$. These are the only maximal ideals.[2.8] This is because:

$$R/(x, y) = \mathbb{C}[x, y]/(x, y) = \mathbb{C} \tag{2.29}$$

which is a field. The fact that these are the only ones is hard to prove.

The prime ideals for this ring are the maximal ideals, (0), and (f) for irreducible polynomials f. This is because $R/(f)$ is an integral domain.[2.9]

Proposition 2.5. *In summary: the following inclusions hold:*

$$\textit{Crings} \supset \textit{ID} \supset \textit{UFD} \supset \textit{PID} \supset \textit{ED} \supset \textit{Fields} \tag{2.30}$$

2.6.1 Zorn's Lemma

We seek to prove that every proper ideal of a ring is contained in some maximal ideal. This might seem obvious, but we actually need some heavy duty machinery to deal with this question.

Definition 2.18 (Maximal)**.** The maximal element of some ordered set is an element $a \in S$ such that there does not exist an element such that $b > a$.

Definition 2.19 (Partial Order)**.** Given a set S, a partial order is a binary relation $\leq : S \times S \to S$ such that for all $x, y, z \in S$, we have:

1. Reflexive: $x \leq x$
2. Transitive: $x \leq y$ and $y \leq z$ implies $x \leq z$
3. Antisymmetric: $a \leq b$ and $b \leq a$ implies $a = b$

[2.8] See Hilbert's Nullstellensantz

[2.9] In algebraic geometry, factoring out maximal ideals gives points, and factoring out irreducible polynomials gives curves. Factoring out (0) gives the plane.

Remark 2.11. It is not always the case that "ordered" sets have a maximal element. Consider $(0, 1)$ this is totally ordered, but has no maximal elements. So how do we actually know a maximal ideal exists?

Remark 2.12. There might be many maximal elements of a set. This is contrary to the concept of maximum, which is the idea that something is greater than every other element.

Lemma 2.2 (Zorn's Lemma)**.** *Consider a nonempty partially ordered set S. If it is the case that every totally ordered subset of S has an upper bound, then we have that S itself has a maximal element.*

Proof. This is a sketch, since the fully rigorous proof requires some set theory beyond the scope of the class. First, we take $s_0 \in S$ since S is nonempty. Then this means $\{s_0\}$ is totally ordered. Therefore we have an upper bound s_1. If s_0 is not maximal, then $s_1 > s_0$.

Repeat this with $\{s_0, s_1\}$ which is also totally ordered. Continue in this fashion infinitely many times.[2.10] At this point we have some upper bound s_ω of $\{s_0, s_1, \cdots\}$. We find some s_α for every ordinal α but the set of ordinals is a proper class, and since S is a set, it is smaller than the class of ordinals. Therefore S is exhausted before the ordinals are and we get a contradiction, and therefore some maximal element. □

Lemma 2.3. *The union of a totally ordered set of ideals of some ring R is also an ideal.*

Proof. Take some totally ordered set of ideals $\{I_\alpha\}$ of a ring R.

If $a, b \in \cup I_\alpha$ then we have that for some α_1, α_2, $a \in I_{\alpha_1}$ and $b \in I_{\alpha_2}$. Since this set is totally ordered by inclusion, we know that one of the two is the case:

$$I_{\alpha_1} \subseteq I_{\alpha_2} \qquad\qquad I_{\alpha_2} \subseteq I_{\alpha_1} \tag{2.31}$$

so WLOG we have take $I_{\alpha_1} \subseteq I_{\alpha_2}$ so $ab \in I_{\alpha_2}$. □

Warning 2.2. This lemma may seem trivial, but we won't always have this for a collection of ideals which is not totally ordered. The issue lies in the union not being closed under addition.

Theorem 2.8. *If I is a proper ideal of some ring R, Then we have that I is contained in some maximal ideal, so there exists a maximal ideal, unless $R = 0$.*

Proof. Assuming Zorn's lemma, we now have to show that the set of all proper ideals of any ring R containing some ideal I satisfies the hypotheses of Zorn's lemma. S is partially ordered by inclusion. It is also nonempty because $I \in S$.

To see every totally ordered subset of S has an upper bound, consider some $\{I + \alpha\}$ which forms a totally ordered subset of S. This means that we have:

$$\bigcup_\alpha I_\alpha \tag{2.32}$$

[2.10] This step technically requires the axiom of choice. As such, Zorn's lemma was controversial at one point in time. It is largely agreed upon today.

is an ideal containing I_β for all β by lemma lemma 2.3. □

Remark 2.13. Besides the proof that every ideal of a ring is contained in some maximal ideal, we have another application of Zorn's lemma.

Corollary 2.1. *The intersection of all prime ideals of a ring is the set of all nilpotent elements of the ring.*

Proof. If $\mathfrak{p}$ is a prime ideal of some ring R. Then $x^n \in \mathfrak{p}$ which means either x^{n-1} or x is in $\mathfrak{p}$. Now we just repeat this for all the multiples of x. This means if x is nilpotent, it is in every prime ideal, and therefore the intersection of every prime ideal.

Now suppose x is not nilpotent. Find a prime ideal not containing x. Now we can use Zorn's lemma to construct prime ideals as well. Define:

$$M \coloneqq \left\{1, x, x^2, \cdots\right\} \not\ni 0 \tag{2.33}$$

because x is not nilpotent. Now let S be the set of ideals disjoint from M. Note S is partially ordered by inclusion. It also happens to be nonempty, since we get $(0) \in S$ for free by the construction of M. We also get an upper bound of every totally ordered subset. Namely the union of the elements. Therefore we have some maximal element I. Note I is only a maximal element in S, and not necessarily a maximal ideal of R.

Now we desire to show that I is prime. Suppose $a, b \notin S$. This means $(I, a) \supsetneq I$ which means it must contain an element of M. Namely:

$$i_1 + sa = x^n \tag{2.34}$$

We have the same situation for (I, b) and therefore have some element of M:

$$i_2 + tb = x^n \tag{2.35}$$

which means:

$$\underbrace{i_1 i_2 + i_1 tb + i_2 sa}_{\in I} + stab = x^{m+n} \in M \tag{2.36}$$

which means $ab \notin I$ because if it were in I, we would have that the entire expression is, which can't be the case because it is in M. This mean I must be prime. □

2.7 Localization

2.7.1 Motivation and Construction

Example 2.25. In $\mathbb{Z}$ we don't have division. To get multiplicative inverses, we add them "manually" and get:

$$\mathbb{Q} = \{m/n \,|\, m, n \in \mathbb{Z}\} \tag{2.37}$$

which is indeed a field.

Definition 2.20 (Quotient ring)**.** Given a cring R, and a multiplicative subset $S \subseteq R$, the field consisting of all elements of S and their multiplicative inverse is called the *quotient ring* and is written $R\left[S^{-1}\right]$.

Example 2.26. If a cring R is an integral domain, and S is the set of all nonzero elements of R, then we have that $R\left[S^{-1}\right]$ is a quotient field of R.

We proceed to construct such an object in the general case. Our construction considers two cases. First the case when we have no zero divisors, and then when we do.[2.11]

Proposition 2.6. *Let R be a commutative ring, $S \subseteq R$. Also let $1 \in S$, and S is multiplicatively closed with no zero divisors. Then the relation*

$$(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_2 \tag{2.38}$$

is an equivalence relation, and the equivalence classes under this relation form a quotient ring $R\left[S^{-1}\right]$.

Proof. Recall that if a, b both have inverses, then ab does as well. Now take all pairs (r, s) such that $r \in R, s \in S$. We define a relation as in the statement of the proposition. Note this is motivated by taking "fractions" just as is done in the specific case of constructing $\mathbb{Q}$ from $\mathbb{Z}$. The subtle point in this construction comes from the fact that we need to check whether this relation satisfies transitivity.

Suppose $(r_1, s_2) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. This means we have:

$$\begin{aligned} r_1 s_2 s_3 &= r_2 s_1 s_3 = r_3 s_1 s_2 & (2.39)\\ \iff 0 &= s_2\left(r_1 s_3 - r_3 s_1\right) & (2.40) \end{aligned}$$

then since we aim to show $r_1 s_3 = r_3 s_1$ (since this would mean $(r_1, s_1) \sim (r_3, s_3)$) we use that there are no zero divisors in our ring R, and therefore have the desired equality. We leave it as an exercise to check the remaining qualities of an equivalence relation, and that the equivalence classes form a ring.

This gives us $R\left[S^{-1}\right]$ as the equivalence classes of this form. Now we have the map $R \to R\left[S^{-1}\right]$ is injective since it has trivial kernel. This is because if $r \mapsto (r, 1)$, then $(r, 1) \sim (0, 1)$ so means $r \cdot 1 = 0 \cdot 1$ so r must be 0 since we have no zero divisors in R. □

Proposition 2.7. *Let R be a commutative ring, $S \subseteq R$ be a multiplicative subset and $1 \in S$. Then if we take $(r_1, s_2) \sim (r_2, s_2)$ iff there exists some $s_3 \in S$ such that:*

$$s_3\left(r_2 s_1 - s_2 r_1\right) = 0 \tag{2.41}$$

this gives us a quotient ring $R\left[S^{-1}\right]$ with the following properties:

[2.11] This differs from the approach in Lang [5] which treats all rings on an equal footing. The idea here is that the two step approach makes the motivation for the general equivalence relation more clear.

1. *There exists a homomorphism from R to $R\left[S^{-1}\right]$.*[2.12]
2. *The image of all elements of S in $R\left[S^{-1}\right]$ are invertible in $R\left[S^{-1}\right]$.*
3. *$R\left[S^{-1}\right]$ is the universal ring with these properties.*

$$\begin{tikzcd}
R \arrow[r] \arrow[dr] & R\left[S^{-1}\right] \arrow[d, dashed] \\
 & X
\end{tikzcd} \tag{2.42}$$

Proof. Note that this proposition does not assume the absence of zero divisors. We can use much of the proof of the previous proposition, if we identify the point where we used that there were no zero divisors, and adapt the equivalence relation accordingly. Namely the proof of the transitivity falls apart.

Take I to be the following:

$$I \coloneqq \{x \in R \,|\, \exists s \in S, xs = 0\} \tag{2.43}$$

This is closed under multiplication, because for two elements $x, y \in I$ we have that $\exists s, t \in S$ such that

$$(x_1 + x_2)\, st = 0 \tag{2.44}$$

and since S is closed under multiplication, we have that $st \in S$ so $x_1 + x_2 \in I$. Now consider R/I, and define $\bar{S}$ to be the image of S in R/I. Now form $R/I\left[\bar{S}^{-1}\right]$ as we did in the non-zero divisor case.

The kernel of the map from R to $R\left[S^{-1}\right]$ is I, the set of elements killed by something in S. This motivates the equivalence relation in the statement of the theorem. □

2.7.2 Examples

We now consider the question of how and what localization actual "localizes."

Example 2.27. This example illustrates how an analyst might answer this question. Consider the ring $R = \mathbb{C}[x]$. In particular, we are interested in what these functions look like "around" $0 \in \mathbb{C}$. We might take the rational functions non-singular at 0.[2.13] As it turns out these comprise the set $R\left[S^{-1}\right]$ where S is the set of polynomials which are not zero at 0. The map from R to $R\left[S^{-1}\right]$ is injective, but not surjective.

Example 2.28. We now provide an example of how an algebraic geometer might answer the question. Consider the ring of all continuous functions on $\mathbb{R}$. Again we focus on 0. Look at the germs of functions at 0. These are the

[2.12] this is only a homomorphism because the injectivity depends on the non-existence of zero divisors.

[2.13] The rational functions are sort of like the "poor man's holomorphic functions" since they are in some sense an approximation. But they are much easier to deal with algebraically.

functions which are equivalent in some neighborhood of 0. The ring of germs is $R\left[S^{-1}\right]$ where S is the set of functions which are nonzero at the origin.

The map from R to $R\left[S^{-1}\right]$ here is surjective but no injective.

Remark 2.14. As in the last two examples, we have the general statement: the complement of a prime ideal $\mathfrak{p}$ is multiplicatively closed.

Example 2.29. We now seek to answer this question from the point of view of a number theorist. Consider the ring $\mathbb{Z}$, and suppose we are interested in the prime ideal (2). Now let $S = \mathbb{Z} \setminus (2)$ which gives us only the odd numbers. This gives us:

$$\mathbb{Z}_{(2)} \coloneqq \{a/b \in \mathbb{Q} \mid b \in S\} \tag{2.45}$$

In general this is $R_p = R\left[S^{-1}\right]$ where S is the complement of (p) in R.

Recall 2 is a prime element of $\mathbb{Z}_{(2)}$. The units of $\mathbb{Z}_{(2)}$ are rationals of the form a/b with both a, b odd. Also note that any element of $\mathbb{Z}_{(2)}$ can be written $2^n u$ for some unique $n \in \mathbb{N}$ and some unit u. We recognize that this is a UFD with the single prime 2. We have essentially killed off all primes besides 2, and therefore this number system is somehow useful to number theorists.[2.14]

Remark 2.15. The elements of the completion of the above construction in example example 2.29 are called the 2-adic numbers. In general these are called the p-adic numbers.

[2.14] For more, see [4].

Chapter 3

Modules

3.1 Definitions

Definition 3.1 (Module)**.** Let A be a ring. A *left module* M over A, also called a *left* A*-module* is an abelian group M, paired with an operation of A on M written $\cdot : A \times M \to M$ which must satisfy the following conditions for all $a, b \in A$ and $x, y \in M$.

1. $(a+b) \cdot x = ax + bx$
2. $a \cdot (x+y) = a \cdot x + a \cdot y$
3. $(ab) \cdot x = a \cdot (b \cdot x)$
4. $1 \cdot x = x$

we define a *right* A*-Module* in a similar way.

Example 3.1. The canonical example of a module is a vector space, which is just a module over a field, rather than a general ring.

Definition 3.2. Let M_1, M_2 be two R-modules. A module homomorphism between M_1, M_2 is a function $f : M_1 \to M_2$ such that for all $m_1 \in M_1$, $m_2 \in M_2$, and $r \in R$ we have

$$f(m_1 + m_2) = f(m_1) + f(m_2) \qquad\qquad f(r \cdot m_1) = r \cdot f(m_1) \tag{3.1}$$

Remark 3.1. It is customary to write all module homomorphisms as "acting" on the left. This is counter-intuitive in light of the condition that elements of r are "associative" with f. It makes more sense to write homomorphisms of left modules on the right, so the condition becomes $(rm)f = r(mf)$ to suggest associativity rather than commutativity. Similarly it makes more sense to write homomorphisms of right modules on the left.

Example 3.2. Let M, N be R-modules. Then the set of homomorphisms from M to N, written, $\operatorname{Hom}_R(M, N)$ is an abelian group. If R is also commutative, then we have that $\operatorname{Hom}_R(M, N)$ is an R-module.

Example 3.3. Given the following exact sequence:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{3.2}$$

we might wonder if the following sequences are exact?

$$\begin{gathered}
0 \longrightarrow \operatorname{Hom}(M, A) \longrightarrow \operatorname{Hom}(M, B) \longrightarrow \operatorname{Hom}(M, C) \longrightarrow 0 \\
0 \longleftarrow \operatorname{Hom}(A, N) \longleftarrow \operatorname{Hom}(B, N) \longleftarrow \operatorname{Hom}(C, N) \longleftarrow 0
\end{gathered} \tag{3.3}$$

First notice, if A, B, C are vector spaces, these are certainly still exact. They also are if B splits as $A \oplus C$, which gives us

$$0 \to A \to A \oplus C \to C \to 0 \tag{3.4}$$

These sequences are, however, not exact in general. See example example 3.4.

Example 3.4. As a counterexample to the sequences in example example 3.3 we consider

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \arrow[r] \arrow[d, equal] & \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \arrow[r] \arrow[d, equal] & \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \arrow[d, equal] \\
 & 0 & 0 & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd} \tag{3.5}$$

$$\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longleftarrow \operatorname{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longleftarrow \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longleftarrow 0$$

Then the left map on the bottom line is not onto, and therefore we cannot have a 0 on the left.

Remark 3.2. The fact that sequences of the sort explored in examples examples 3.3 and 3.4 are not generally exact leads to the field of homological algebra.

3.2 Examples

Example 3.5. As mentioned earlier, vector spaces are modules over fields.

Example 3.6. Abelian groups are modules over $\mathbb{Z}$.

Example 3.7. Left ideals of a ring R are the same as left submodules of a module R.

Example 3.8. Let G be a group which acts on a set S. We can form a vector space V with basis S. Now we can let G act on V in the obvious way. Then considering the group ring $K[G]$, this has basis G, and is clearly a ring. Then V is a module over the ring $K[G]$. This is an important example in representation theory.

Definition 3.3 (Bimodule)**.** A module M is a *bimodule* over two rings, iff it is a left module over one ring, and right module over another, and the actions commute with one another.

Example 3.9. Let M be a left module over a ring R. Then consider the module endomorphisms $\mathrm{Hom}_R(M, M)$ also written $\mathrm{End}(M)$. This is a ring, where the product is given by composition. Then we have that M is a right module over $\mathrm{End}(M)$. The right action of $\mathrm{End}(M)$ commutes with the left action of R on M.[3.1]

Remark 3.3. $\mathrm{End}(M)$ is analogous to $\mathrm{Perm}(S)$. If we have a group, we often consider its representation as $\mathrm{Perm}(S)$ for some set S. Similarly, one often considers a ring as a subring of $\mathrm{Hom}_T(M, M)$ for some T-module M.

Example 3.10. Let R be a ring. Then R is an (R, R) bimodule.

Example 3.11 (Algebraic Number Theory)**.** Take some algebraic number field $\mathbb{Q}[i]$ where $i^2 = -1$. Think of $\mathbb{Q}[i]$ as a vector space over $\mathbb{Q}$ where the elements $\mathbb{Q}[i]$ are the endomorphisms of the vector space. Therefore elements of $\mathbb{Q}[i]$ can be represented as matrices. Matrices are linear transformations of a vector space and in effect homomorphisms of modules. Therefore we pick a basis of $\mathbb{Q}[i]$, namely $\{1, i\}$ and now we see:

$$1 : 1 \to 1, \qquad 1 : i \to i, \qquad i : 1 \to i, \qquad i : i \to -1 \tag{3.6}$$

so we have the matrix representations:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad q = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \tag{3.7}$$

for arbitrary $q \in \mathbb{Q}[i]$.

We can look at the invariants of these matrices. These are the usual tr and det. In this context the determinant is sometimes called the norm. Namely the trace of an element $a + bi$ is $2a$, and the norm is $a^2 + b^2$.

3.3 Free modules

Definition 3.4 (Direct Sum of Modules)**.** The *direct sum* of a collection of modules $\{M_\alpha\}_{\alpha \in A}$ is given by $\bigoplus_\alpha M_\alpha$ which is an abelian group with a corresponding action by R given by the component-wise action on M_α.

[3.1] This is similar to when we considered the action of a group on itself.

Definition 3.5 (Free Module)**.** A module is a *free module* iff it is a sum of copies of a ring R. This is often written R^n.

Example 3.12. All vector spaces are free modules.

Example 3.13. $\mathbb{Z}$ is a free module over $\mathbb{Z}$. $\mathbb{Z}/2\mathbb{Z}$ is not free.

Example 3.14. We might wonder whether we can define the rank of a free module in a meaningful way, that is if $R^m \simeq R^n$ does this mean $m = n$? We first notice that this is not the case for the trivial ring $\{0\}$. So clearly not in general. What about other cases?

Claim 3.1. If we have that $R^m \simeq R^n$ we have that $n = m$ if R is a field.

Theorem 3.1. *Let R be a non-trivial cring. Then if $R^m \cong R^n$ we have that $n = m$.*

Proof. Pick maximum ideal I in R. This exists since R is non-trivial. We can then notice that

$$(R/I)^m \cong (R/I)^n \tag{3.8}$$

as modules over the field R/I meaning $m = n$ by claim 3.1. □

Warning 3.1. The preceding theorem is only sometimes true for non-commutative rings.

Example 3.15. If we take $R = M_n(K)$ (the $n \times n$ matrices over some field K) where $R^a \simeq R^b$, then we have that these are vector spaces over the same field with ranks an^2, bn^2 and therefore $a = b$ so we have the same conclusion as theorem theorem 3.1. R is, however, non-commutative.

Example 3.16. We consider now a ring R which splits as $R \oplus R$ as R-modules. Consider the set $\operatorname{Hom}(R^m, R^n)$. This can be identified with $m \times n$ matrices. The counter-intuitive aspect of this example is that if we do have $R = R \oplus R$, this means there is some 1×2 (and therefore non-square) invertible matrix.

Pick some abelian group A such that $A \simeq A \oplus A$. An example of this is $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$. If we take $R = \operatorname{End}(A)$ we get our desired ring. This is the set of infinite matrices where each row has all but a finite number of its entries as zero. This means $R = \operatorname{Hom}(A, A) = \operatorname{Hom}(A, A \oplus A) = R \oplus R$.

3.4 Projective modules

Definition 3.6 (Adjunction)**.** Let $\mathbf{A}, \mathbf{B}$ be categories. An *adjunction* from $\mathbf{A}$ to $\mathbf{B}$ is a triple $\langle F, G, \varphi \rangle : \mathbf{A} \rightharpoonup \mathbf{B}$ where F, G are functors such that:

$$\begin{tikzcd} \mathbf{A} \arrow[r, shift left, "F"] & \mathbf{B} \arrow[l, shift left, "G"] \end{tikzcd} \tag{3.9}$$

and φ is a function bringing pairs (a, b) for $a \in \operatorname{Obj}(\mathbf{A})$ and $b \in \operatorname{Obj}(\mathbf{B})$ to a bijection

$$\varphi_{a,b} : \operatorname{Mor}(Fa, b) \cong (a, Gb) \tag{3.10}$$

which is natural in x, a. The functors F, G are also said to be *adjoint*.

Definition 3.7 (Projective Modules)**.** A module is a *projective module* iff it satisfies the following property: Given that $M \to N \to 0$ it exact, map $P \to N$ lifts to some unique map $P \to M$. In other words we have the following diagram:

$$\begin{tikzcd}
M \arrow[r] & N \arrow[r] & 0 \\
 & P \arrow[u] \arrow[ul, dashed] &
\end{tikzcd} \tag{3.11}$$

Remark 3.4. This definition is directly satisfied by free modules, and we therefore see that projective modules are effectively a slight variation of free modules.

Proposition 3.1. *All free modules are projective.*

Proof. Let M be a module. Just as we did with groups and rings, we can construct a category of Modules over a ring R. We can then consider a forgetful functor F from this category into **Set**. This gives us an association between M and some associated set S_M. We then have a notion of a functor G going in the other direction, and forming a free module with basis S, written M_S. We then have the following commuting diagram:

$$\begin{tikzcd}
M \arrow[r, "F"] \arrow[d, "f"] & S_M \arrow[d, "F(f)"] \\
N & S_n \arrow[l, "G"']
\end{tikzcd}$$

The functors F, G are then called adjoint. This means all free modules are projective. □

Lemma 3.1. *The following are equivalent:*

1. *P is projective*
2. *There exists some module Q such that $P \oplus Q$ is free.*

Proof. (1) $\implies$ (2): Pick some free module F such that we have $\psi : F \to P$ onto. Then we have $F \to P \to 0$ exact. Therefore we can lift $P \to F$. The diagram here is:

$$\begin{tikzcd}
F \arrow[r, "\psi"] & P \arrow[r] & 0 \\
 & P \arrow[u, "\mathrm{id}"] \arrow[ul, dashed] &
\end{tikzcd} \tag{3.12}$$

But then we have that $F = P \oplus \ker(\varphi)$.

(2) $\implies$ (1): We leave this direction as an exercise. □

Remark 3.5. This is meant to allow us to check when a module is projective and not free.

Example 3.17. Consider $R = \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ so we have that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are both projective over $\mathbb{Z}/6\mathbb{Z}$ but not free.

Example 3.18 (Möbius Strip)**.** The möbius strip corresponds to a projective module which is not free, whereas a regular cylindrical strip corresponds to a free module.

To see this consider S^1 and take R to be the continuous functions on S^1. We can then take $M = R$ and think of M as functions mapping $S^1 \to S^1 \times \mathbb{R}$ such that $f(s)$ lies above S^1. Note M is free. Then we regard M as the *sections* of $S^1 \times \mathbb{R} \to S^1$. This is what is knows as a *vector bundle.* An assignment of a vector space to each point in S^1.

The Möbius strip can be viewed as a vector bundle over S^1. This means that each fibre is isomorphic to $\mathbb{R}$. Now if we take N to be the sections of this twisted vector bundle, we see that N is projective but not free.

The orientations of the fibres clearly change as you go around S^1. This makes N projective, since $N \oplus N = M \oplus M$. Considering the normal bundle at each point of S^1, it is clear that we get an orthogonal band by taking the orthogonal complement at each point. We then have two bands which have fibres that intersect at each point of S^1. This allows us to think of $N \oplus N$ as the sum of two Möbius strips.

In general this allows us to think of projective modules which are not free, as twisted versions of free modules.

Example 3.19. Consider the ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$. This has a natural interpretation as a rectangular lattice in $\mathbb{C}$. The principal ideals are rectangular with respect to the whole lattice, and the non-principal ideals lie in a diamond shape. Principal ideals are free modules, and non-principal ideals are not.

We can consider the module $M = \left(2, 1 + \sqrt{-2}\right)$. We wish to show that M is projective. Consider the onto map: $gR \oplus R \to M$ which sends $(1,0) \mapsto 2$, and $(0,1) \mapsto 1 + \sqrt{-5}$. We now construct a section $f : M \to R \oplus R$ such that $g(f(m)) = m$. So $R \oplus R = M \oplus \ker(g)$.

$$f(x) \coloneqq \left(-x, x\frac{1+\sqrt{-5}}{2}\right) \tag{3.13}$$

and check that $f(x) \in R \oplus R$. This shows M is projective.

Example 3.20. We given an example illustrating a submodule of a free module which is not a projective module. Let K be a field, then we can consider the ring of polynomials $R = K[x,y]$. Now consider the ideal $I = (x,y)$. This is the set of all polynomials with no constant term. In particular, this is a submodule of some free module R. We want to show this is not projective. To see this, look at

$$\begin{tikzcd} R \oplus R \arrow[r, "g"] & I \arrow[r] & 0 \\ (1,0) \arrow[r, mapsto] & x & \\ (0,1) \arrow[r, mapsto] & y & \end{tikzcd} \tag{3.14}$$

First note that this map is onto. If I is projective, then there exists a unique map $f : I \to R \oplus R$ such that $g\left(f\left(a\right)\right) = a$ for all $a \in I$. The diagram here is:

$$\begin{tikzcd}
R \oplus R \arrow[r, "g"] & I \arrow[r] & 0 \\
& I \arrow[u, equal] \arrow[ul, dashed]
\end{tikzcd} \tag{3.15}$$

Suppose

$$f\left(x\right) = \left(a, b\right) \in \mathbb{R}^2 \qquad\qquad f\left(y\right) = \left(c, d\right) \in \mathbb{R}^2 \tag{3.16}$$

which means $ax + by = x$ and $cx + dy = y$. This implies $a = 1 + x \times \bullet$ But this cannot coincide with $y\left(a, b\right) = x\left(c, d\right)$ since this would mean $ya = xc$, $yb = xd$ which means $ya = xc$ which implies $a \neq q + y \times \bullet$ as desired.

Proposition 3.2. *An infinite sum can often be regrouped in two different ways to give two different values. This is called the* Eilenberg-Mazur swindle*. It is only valid when:*

1. *The elements in question have additive inverses*
2. *All infinite sums in question are well defined*

Example 3.21 $(1 = 0)$**.** There is a common "proof" that $1 = 0$. It goes as follows: Consider the sum:

$$1 - 1 + 1 - 1 \cdots \tag{3.17}$$

now we can group this in two ways. We can consider:

$$1 + \left(-1 + 1\right) + \left(-1 + 1\right) + \cdots = 1 \tag{3.18}$$

or we can consider

$$\left(1 - 1\right) + \left(1 - 1\right) + \cdots = 0 \tag{3.19}$$

This is an improper use of the Eilenberg-Mazur swindle from proposition 3.2 since the sums in question are not well defined.

Example 3.22. We can apply the swindle from proposition 3.2 in algebraic topology. In particular, we can consider knots. We can consider cancelling knots and just attach them together. The infinite sum here corresponds to adding increasingly small knots on to the string in increasingly close intervals.

Example 3.23. Let P be a projective module. Then we have that there exists some module Q such that $P \oplus Q = F$ where F is free. The module Q is also projective then. In addition, we can take Q free (in fact even equal to F). If we think of free modules as "ignorable," since we have $P \oplus Q$ is free, we are in an analogous situation to having an additive inverse. In particular, we have well define infinite sums, and some sense of additive inverses, so we can apply the swindle in proposition 3.2. In other words,

$$\begin{aligned} P &= P \oplus \left(Q \oplus P\right) \oplus \left(Q \oplus P\right) \cdots & (3.20) \\ &= \left(P \oplus Q\right) \oplus \left(P \oplus Q\right) \oplus \cdots & (3.21) \end{aligned}$$

must be free. The catch is that Q is often times not finitely generated.

3.5 Tensor products

3.5.1 Construction

Definition 3.8 (Bilinear map)**.** Let $f : X \times Y \to Z$. This is a *bilinear map* iff $f(x, \cdot)$ is linear for fixed x, and $f(\cdot, y)$ is linear for fixed y.

Definition 3.9 (Tensor Product)**.** Let R be a commutative[3.2] ring, and M, N, P R-modules. A module is the tensor product $M \otimes N$ iff it is the module such that given a bilinear map $f : M \times N \to P$ there exists a linear map $g : M \otimes N \to P$ making the following diagram commutative:

$$\begin{tikzcd}
M \times N \arrow[r, "otimes"] \arrow[dr, "f"] & M \otimes N \arrow[d, dashed, "g"] \\
& P
\end{tikzcd} \tag{3.22}$$

Example 3.24. Given two modules M, N we now consider how to construct the tensor product $M \otimes N$. First consider the free modules on the objects $m \otimes n$ where $m \in M$ and $n \in N$. This gives is linear maps bringing this free modules to P. This is written $m \otimes n \mapsto f(m, n)$. We then quotient out certain undesirable elements:

$$(m_1 + m_2) \otimes n - m_1 \otimes n - m_1 \otimes n \tag{3.23}$$

$$m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2 \tag{3.24}$$

$$(rm) \otimes n - r(m \otimes n) \tag{3.25}$$

$$m \otimes (rn) - r(m \otimes n) \tag{3.26}$$

This kills the elements that prevent the desired relationships, such as

$$(rm) \otimes n = r(m \otimes n) = m \otimes (rn) \tag{3.27}$$

This shows the generic existence of the tensor product.

Example 3.25. What does the tensor product look like? We know that:

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N) \tag{3.28}$$

so some bilinear map brings $(M_1 \oplus M_2) \otimes N \to P$ which is somehow the same as a pair of bilinear maps from $(M_1 \otimes N)$ to P, and $(M_2 \otimes N)$ to P. We also know that

$$R \otimes M \simeq M \tag{3.29}$$

so we have that a bilinear map bring $R \times M$ to P is the same as linear maps from $M \to P$.

Example 3.26. We can show that:

$$\mathbb{R}^n \otimes \mathbb{R}^m \simeq \mathbb{R}^{mn} \tag{3.30}$$

If V, W are vector spaces with basis $\{v_i\}, \{w_i\}$ then $V \otimes W$ has basis $\{v_i \otimes w_j\}$.

[3.2] We don't need this assumption, but it helps to understand the concept here first, and then return to consider the general case.

3.5.2 Exact sequences

Lemma 3.2. *Let A, B, C be modules. The sequence $A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact iff*

$$\operatorname{Hom}(A, M) \longleftarrow \operatorname{Hom}(B, M) \longleftarrow \operatorname{Hom}(C, M) \longleftarrow 0 \tag{3.31}$$

is exact.

Proof. We leave this as an exercise. □

Proposition 3.3. *Let M be a module, and let $A \to B \to C \to 0$ be exact. This implies that the following sequence is also exact:*

$$A \otimes M \longrightarrow B \otimes M \longrightarrow C \otimes M \longrightarrow 0 \tag{3.32}$$

We say that $\otimes M$ is right exact*.*

Remark 3.6. Note that the first map in the sequences in the preceding example is not necessarily injective. In other words we can't put a 0 on the left in the general case.

Remark 3.7. Proving things with regard to tensor products should usually have to do with universality rather than the construction using relations and objects.

Proof. Note first that elements of $\operatorname{Hom}(A \otimes B, C)$ are bilinear maps from $A \times B$ to C, which are linear maps from A to $\operatorname{Hom}_R(B, C)$. This is analogous to the situation in **Set** where functions bringing $R \times S$ to T are the same as functions bringing $R \to \operatorname{Mor}(S, T)$.

We want to show that $A \otimes N \longrightarrow B \otimes N \longrightarrow C \otimes N \longrightarrow 0$ is exact. So using lemma 3.2 we just have to show that:

$$\operatorname{Hom}(A \otimes N, M) \leftarrow \operatorname{Hom}(B \otimes N, M) \leftarrow \operatorname{Hom}(C \otimes N, M) \leftarrow 0 \tag{3.33}$$

But we also have a relationship between homomorphisms $A \otimes N \to M$ and linear maps $A \to \operatorname{Hom}_R(N, M)$ which means it is sufficient to show the following sequence is exact:

$$\begin{tikzcd}
\operatorname{Hom}(A, \operatorname{Hom}(N, M)) & \operatorname{Hom}(B, \operatorname{Hom}(N, M)) \arrow[l] \arrow[dl, rounded corners] \\
\operatorname{Hom}(C, \operatorname{Hom}(N, M)) & 0 \arrow[l]
\end{tikzcd} \tag{3.34}$$

which is again exact by lemma 3.2. □

Example 3.27. We are now in a position to calculate particular tensor products. Take the following sequence $R^a \longrightarrow R^b \xrightarrow{f} M \longrightarrow 0$ where R^a, R^b are free modules. Then pick a relations generating $\ker(f)$ and pick a set of b generators of M. Taking the tensor product with N gives us the exact sequence

$$R^1 \otimes N \longrightarrow R^b \otimes N \longrightarrow M \otimes N \longrightarrow 0 \tag{3.35}$$

so we have the sequence

$$N^a \longrightarrow N^b \longrightarrow M \otimes N \longrightarrow 0 \tag{3.36}$$

which implies $M \otimes N = N^b / \operatorname{im}\left(N^a - N^b\right)$.

Example 3.28. Now we desire to find $M \otimes N$ for finitely generated abelian groups M, N. Recall these are also $\mathbb{Z}$ modules, in the sense that they can be expressed as direct sums of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. Now since we know that $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$ we can just work out a few examples:

1. $\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}$
2. $\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$
3. $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$
4. $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\gcd(m,n)\,\mathbb{Z}$

The last line is the only result worth mentioning. To find this, we consider the following exact sequence:

$$\mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0 \tag{3.37}$$

and therefore we also have the following exact sequence:

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}) \longrightarrow 0 \tag{3.38}$$

so we have

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n/ZZ)\,/m\,(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\gcd(m,n)\,\mathbb{Z} \tag{3.39}$$

Example 3.29.

$$\begin{aligned}
\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} &= \mathbb{Z}/2\mathbb{Z} && (3.40)\\
\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} &= 0 && (3.41)\\
\mathbb{Z}/9\mathbb{Z} \otimes \mathbb{Z}/12\mathbb{Z} &= \mathbb{Z}/3\mathbb{Z} && (3.42)
\end{aligned}$$

We see here that the tensor product fails to be left exact. Considering

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\times 2"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{3.43}$$

the bottom line then is not exact.[3.3]

[3.3] This is somewhat of a nuisance according to professor Borcherds. It also leads to the notion of cohomology.

Definition 3.10 (Algebra)**.** A cring S is an *algebra* over a ring R iff it is paired with a homomorphism $R \to S$ which makes S an R-module. If this is associative, S is a called an *associative algebra*.

Remark 3.8. Algebras are effectively modules with multiplication.

Definition 3.11. An algebra S over a ring R is a division algebra iff it is nontrivial, and for any $a \in S$ and nonzero $b \in S$, there exists exactly one element $s \in S$ such that $a = bs$ and exactly one elements $t \in S$ such that $a = tb$. Note if S is an associative algebra, then S is a division algebra iff it has a multiplicative identity $1 \neq 0$ and every nonzero element of S has a multiplicative inverse.

Example 3.30. Let S, T be algebras over a ring R. Then consider $S \otimes_R T$. This is a push-out of S, T over R. As such, we have the following diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & S \arrow[d] \\ T \arrow[r] & S \otimes_R T \end{tikzcd} \tag{3.44}$$

We first have to check that $S \otimes_R T$ is a cring. In particular we need to define a product on it. That is, a bilinear map from $(S \otimes T) \times (S \otimes T) \to (S \otimes T)$. As we have seen, this is also a homomorphism $S \otimes T \otimes S \otimes T \to S \otimes T$. This depends on the tensor product being associative:

$$(A \otimes B) \otimes C \simeq A \otimes (B \otimes C) \tag{3.45}$$

because maps from each to M are trilinear maps $A \times B \times C \to M$. We have a map $S \otimes S \to S$ given by the product on S itself, and the same for T. This gives us our map from $S \otimes T \otimes S \otimes T \to S \otimes S \otimes T \otimes T \to S \otimes T$ by sending

$$(s_1 \otimes t_2) \times (s_2 \otimes t_2) \to s_1 s_2 \otimes t_1 t_2 \tag{3.46}$$

We leave it as an exercise to verify this is actually a pushout.

Example 3.31. Take $S = K[x]$ and $T = K[y]$ with bases $\{x_m\}$ and $\{y^n\}$. Then we have that $S \otimes_R T$ has a basis $\{x^m \otimes y^n\}$. This can be identified with the polynomial ring $K[x, y]$. This map is $x^m \otimes y^n \to x^m y^n$.

Example 3.32. We now show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a ring. First note that $\mathbb{C}$ has a basis $\{1, i\}$. This means $\mathbb{C} \otimes \mathbb{C}$ has a basis:

$$\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\} \tag{3.47}$$

Calculating products we get:

$$\begin{aligned} (i \otimes i)(i \otimes i) &= i^2 \otimes i^2 = 1 \otimes 1 && (3.48) \\ (1 \otimes 1)(a \otimes b) &= (a \otimes b) && (3.49) \\ (1 \otimes 1 + i \otimes i)^2 &= r(1 \otimes 1 + i \otimes i) && (3.50) \end{aligned}$$

This means for $e :- (1 \otimes 1 + i \otimes i)/2$ we have that $e^2 = e$, or that e is idempotent.

This means this ring actually splits as a product. Explicitly,

$$\mathbb{C} \otimes \mathbb{C} = e\,(\mathbb{C} \otimes \mathbb{C}) \times (1-e)\,\mathbb{C}\,(\mathbb{C} \otimes \mathbb{C}) \simeq \mathbb{C} \times \mathbb{C} \tag{3.51}$$

Example 3.33. Recall the axioms of a ring. In particular, the notion of a semiring. In other words, there is no subtraction. Now note the properties satisfied by the tensor product:

1. $(A \otimes B) \otimes C$
2. $(A \oplus B) \otimes C \simeq (A \otimes C) \oplus (B \otimes B)$
3. $A \otimes B \simeq B \otimes A$
4. $A \oplus B \simeq B \oplus A$
5. $(A \oplus B) \oplus C \simeq A \oplus (B \oplus C)$
6. $R \otimes A \simeq A$

This shows us that we fall short in the following ways:

1. The set of all modules is actually a class of modules.
2. There is no effective subtraction.
3. By the swindle, $M = 0$ for all M.

We can deal with number 2 by forcing the set of all pairs $M - N$ for all M, N under some appropriate equivalence relation. We can get also get around 1,3 by considering only the finitely generated modules. This restricts us to an appropriately sized set, and also gets rid of the well definition for infinite sums.[3.4]

Remark 3.9. This leads to the field of K-theory. This concerns taking a ring, and making a ring out of the finitely generated modules of that ring.

Example 3.34. Let $R = \mathbb{Z}$. The finitely generated modules of the integers are all of the form:

$$\mathbb{Z}^n \otimes (\mathbb{Z}/2\mathbb{Z})^{n_2} \oplus (\mathbb{Z}/4\mathbb{Z})^{n_4} \oplus \cdots \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus \cdots \tag{3.52}$$

this gives us a basis $n_i b_i$ where n_i can be positive or negative. The product given by $b_0 \times b_n = b_n$ $b_{p^a} \times b_{p^b} = b_{p^{\min(a,b)}}$

[3.4] This is an exact analogue of the Burnside ring in example 2.5

3.5.3 Noncommutative rings

If we let R be a noncummatative ring, the notion of a tensor product $M \otimes_R N$ is only defined for a right module M and left module N.

Example 3.35. Recall that we need:

$$(mr) \otimes n = m \otimes (rn) \tag{3.53}$$

Next we notice that $M \otimes_R N$ is only an abelian group rather than an R-module. We have:

$$mr \otimes n = m \otimes rn \tag{3.54}$$

which leads to

$$mrs \otimes n = m \otimes srn \tag{3.55}$$

but we want:

$$m\,(rs) \otimes n = m \otimes (rs)\,n \tag{3.56}$$

3.6 Duality

3.6.1 Definition and examples

Definition 3.12. Let M be a module over a ring R. The *dual* of M, written M^*, is the set $\mathrm{Hom}_R\,(M, R)$. M is called the *dualizing object*.

Example 3.36. Let V be a vector space over a field k. Then the dual of V is

$$V^* = \mathrm{Hom}\,(V, k) \tag{3.57}$$

The double dual then is

$$V^{**} = \mathrm{Hom}\,(V^*, k) = \mathrm{Hom}\,(\mathrm{Hom}\,(V, k)\,, k) \tag{3.58}$$

Note k is the *dualizing object* here.

Theorem 3.2. *If $V = \bigoplus_{n=1}^{\infty} k$ then the dimension of V is countable, but the dimension of V^* is uncountable.*

Theorem 3.3. *Let M be a module, over a ring R. There is a natural isomorphism from a module to its double dual given by*

$$m \mapsto (f \to f\,(v)) \tag{3.59}$$

for $m \in M$ and $f \in \mathrm{Hom}\,(M, R)$.

Example 3.37. There is a natural isomorphism from any vector space V to its double dual V^{**}.

Example 3.38. Let $M \cong \mathbb{R}^n$ then we also have $M^* \cong M$. The proof of this is much the same as the case with vector spaces.

Proposition 3.4. *Let M be a projective module. Then $M^* \cong M$.*

Proof. $M \oplus N$ is free, so duality holds for $M \oplus N$ which means duality holds for M. □

Example 3.39. Consider finite abelian groups. These are modules over $\mathbb{Z}$, so it might seem reasonable to choose $\mathbb{Z}$ as the dualizing object. As it turns out this is not useful, because there are no homomorphisms from G to $\mathbb{Z}$ so we are better off taking $\mathbb{Q}/\mathbb{Z}$ to be the dualizing object. We check that $G \cong G^{**}$. To see this, we have that $G = \oplus_i C_i$ for some cyclic groups C_i. Therefore it is sufficient to check this for a cyclic group $G = \mathbb{Z}/n\mathbb{Z}$. Then

$$\mathrm{Hom}\left(G, \mathbb{Q}/\mathbb{Z}\right) \cong \left\{0, \frac{1}{n}, \frac{1}{n}, \cdots, \frac{n-1}{n}\right\} \tag{3.60}$$

would be isomorphic to the set of elements of order n in $\mathbb{Q}/\mathbb{Z}$.

3.6.2 Dirichlet characters

Definition 3.13 (Dirichlet characters)**.** The elements of $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ are called *Dirichlet characters* and are denoted by $\left\{\chi_i\right\}_i$.

Example 3.40. Replace the dualizing object $\mathbb{Q}/\mathbb{Z}$ by

$$S^1 = \{z \in \mathbb{C} : |z| = 1\} \tag{3.61}$$

This doesn't cause any problems because we have the map from $\mathbb{Q}/\mathbb{Z}$ to S^1 given by

$$x \mapsto e^{2\pi i x} \tag{3.62}$$

so $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the elements of finite order in S^1.

Example 3.41. For $n = 8$, we have that

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \{1, 3, 5, 7\} \tag{3.63}$$

Note that $1 = 3^2 = 5^2 = 7^2$ so all elements have the same order. Now we have:

	1	3	5	7
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1

These were of interest to Dirichlet for defining the Dirichlet L-function:

$$\sum_{n \geq 1} \frac{\chi\left(n\right)}{n^s} \tag{3.64}$$

where χ is a Dirichlet character. When $n = 1$ and χ is trivial we get the Riemann ζ-function:

$$\zeta\left(s\right) = \frac{1}{1^s} + \frac{1}{2^s} + \cdots \tag{3.65}$$

Theorem 3.4. *Suppose $\chi_1 \neq \chi_2$. Then we have an inner product of characters given by*

$$(\chi_1, \chi_2) :- \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi_1(x)\overline{\chi_2(x)} = 0 \tag{3.66}$$

Remark 3.10. Note that χ_1 is a complex function on $(\mathbb{Z}/n\mathbb{Z})^\times$ meaning this is essentially a sesquilinear form on a Hilbert space.

Proof. Assume $\chi_1 \neq \chi_2$. Then taking the homomorphism $\chi :- \chi_1\chi_2$ we have that $(\chi_1, \chi_2) = (\chi, 1)$ where 1 is the trivial character which sends everything to 1. Then since $\chi_1 \neq \chi_2$ we have that $\chi \neq 1$, so if we have $a \in \mathbb{Z}/n\mathbb{Z}$ and $\chi(a) \neq 1$, then we can write

$$\sum_{z \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(x) = \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^*} \chi(ax) = \chi(a) \sum_{x \in (\mathbb{Z}/n\mathbb{Z})} \chi(x) \tag{3.67}$$

The multiplication by our element a just re-indexes the elements of $\mathbb{Z}/n\mathbb{Z}$. So together we have:

$$(\chi_1, \chi_2) = (\chi, 1) = \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^\times} \chi(x) = 0 \tag{3.68}$$

□

3.6.3 Fourier transforms

Definition 3.14. Let f be a complex valued function on a finite group G. A function $\tilde{f}$ on G^* is a *Fourier transform* iff it is defined to be:

$$\tilde{f}(\chi) = (\chi, f) = \sum_{x \in G} \chi(x) f(x) \tag{3.69}$$

Proposition 3.5. *Duality for infinite abelian groups (with a topology) have the following characteristics:*

1. *The dualizing object is S^1.*
2. *All groups should be locally compact.*
3. *Homomorphisms should be continuous.*

Example 3.42. Let $G = \mathbb{Z}$. Then we have $G^* = \operatorname{Hom}\left(\mathbb{Z}, S^1\right) \cong S^1$. Now let $H = S^1$. Then H^* is the set of continuous homomorphisms from S^1 to itself given by

$$z \mapsto z^n, n \in \mathbb{Z} \tag{3.70}$$

G, H are dual to one another.

The Fourier transform in this setting takes a function on S^1 to a Fourier series (a function on $\mathbb{Z}$) given by the following:

$$f \mapsto \sum_n c_n \exp\left(2\pi i n z\right), \qquad c_n = \int_{x\in S^1} \exp\left(-2\pi i n z\right) f\left(z\right) dz \tag{3.71}$$

If we have $G = \mathbb{R}$, then $G^* = \operatorname{Hom}\left(\mathbb{R}, S^1\right) \cong \mathbb{R}$. This gives the Fourier transform on $\mathbb{R}$.

3.6.4 Injective modules

Definition 3.15 (Injective module)**.** A module I is an *injective module* iff we have that a sequence $0 \to B \to A$ being exact implies that any map $B \to I$ induces a homomorphism $A \to I$. The diagram is:

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] \\ & I & \end{tikzcd} \tag{3.72}$$

Remark 3.11*.* This definition is "dual" to the concept of a projective module. It is however not obvious how one might find an injective module at all. The first step is however finding a divisible abelian group.

Definition 3.16 (Divisible)**.** A group G is *divisible* iff given some $g \in G$ and some $n \in \mathbb{Z}^+$, there exists some $h \in G$ such that $nh = g$.

Example 3.43. The group $\mathbb{Q}/\mathbb{Z}$ is divisible.

Example 3.44. Finitely generated abelian groups are never divisible, except for the trivial group.

Lemma 3.3. *Let I be some module. If it is a divisible abelian group, then it is an injective module.*

Proof. Pick some $a \in A$ where $a \notin B$. Then we wish to extend f to a. Take the smallest value of $n > 0$ such that $na \in B$. Unless n does not exist. Then we get the desired extension by taking $f\left(a\right) = g$, for $g \in I$ such that $ng = f\left(x\right)$. If we have no such n, then we simply take $f\left(a\right)$ to be anything. Now extend f to all of A (using Zorn's lemma 2.2) by choosing the maximal extension from submodules of A to I. □

Lemma 3.4. *Every abelian group is contained in some injective module.*

Proof. By lemma lemma 3.3 we have that $\mathbb{Q}/\mathbb{Z}$ is injective, and given an abelian group G with an element $a \neq 0$ in G there is some homomorphism f bringing G to $\mathbb{Q}/\mathbb{Z}$ where $f\left(a\right) \neq 0$. Therefore any abelian group G is a subset of a possibly infinite product of copies of $\mathbb{Q}/\mathbb{Z}$. □

Lemma 3.5. *Let R be a ring. Then R^* is an injective R-module.*

Proof. The key point here is that $\mathrm{Hom}_{\mathbb{Z}}\left(R, \mathbb{Q}/\mathbb{Z}\right)$ is an injective R-module. This is by definition the dual of R as a $\mathbb{Z}$-module.

Warning 3.2. $\mathbb{Q}/\mathbb{Z}$ us a $\mathbb{Z}$-module, but not necessarily an $\mathbb{R}$-module.

If we have $f \in \mathrm{Hom}\left(R, \mathbb{Z}\right)$ and $r, s \in R$, then define fr by $fr\left(x\right) = f\left(rs\right)$. Therefore $\mathrm{Hom}_{\mathbb{Z}}\left(R, \mathbb{Q}/\mathbb{Z}\right)$ is a right R-module.

The other key point of the proof is that

$$\mathrm{Hom}_R\left(M, \mathrm{Hom}\left(R, \mathbb{Q}/\mathbb{Z}\right)\right) \cong \mathrm{Hom}_{\mathbb{Z}}\left(M, \mathbb{Q}/\mathbb{Z}\right) \tag{3.73}$$

We leave this as an exercise.[3.5] Now finding an induced homomorphism from A to $\mathrm{Hom}\left(R, \mathbb{Q}/\mathbb{Z}\right)$, is the same as finding an induced homomorphism from A to $\mathbb{Q}/\mathbb{Z}$ which we are guaranteed given that $\mathbb{Q}/\mathbb{Z}$ is injective.

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] & & 0 \arrow[r] & B \arrow[r] \arrow[d] & C \arrow[dl, dashed] \\
& \mathrm{Hom}\left(R, \mathbb{Q}/\mathbb{Z}\right) & & = & & \mathbb{Q}/\mathbb{Z} &
\end{tikzcd} \tag{3.74}$$

So $R^{*}\,\mathrm{Hom}\left(R, \mathbb{Q}/\mathbb{Z}\right)$ is injective as desired. □

Theorem 3.5. *Every module is a submodule of some injective module.*

Remark 3.12. This is analogous to the idea that every module is the quotient of some free module.

3.7 Limits, colimits

3.7.1 Definitions, examples

We recall some useful definitions which we saw in section 1.13 on category theory.

Definition 3.17 (Colimit)**.** Let $\mathcal{A}$ be a category and I a small category. Let $D : I \to \mathcal{A}$ be a diagram in $\mathcal{A}$, and write D^{op} for the corresponding functor $I^{\mathrm{op}} \to \mathcal{A}^{\mathrm{op}}$. A *cocone* on D is a cone on D^{op} and a colimit of D is a limit of D^{op}.

Example 3.45. If we have $G_i \to G_{i+1}$ if we have a limit of these objects we call it G, and have the diagram:

$$\begin{tikzcd}
G_0 \arrow[r] \arrow[drr] & G_1 \arrow[r] \arrow[dr] & G_2 \arrow[r] \arrow[d] & G_3 \arrow[r] \arrow[dl] & \cdots \arrow[dll] \\
& & G & &
\end{tikzcd} \tag{3.75}$$

In this situation G is more or less the union of the G_i.

[3.5] This is easy, but messy to write out.

Example 3.46. $\mathbb{Q}/\mathbb{Z}$ is the union of

$$\mathbb{Z}/\mathbb{Z} \subseteq \left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z} \subseteqq \left(\frac{1}{6}\mathbb{Z}\right)/\mathbb{Z} \subseteq \left(\frac{1}{24}\mathbb{Z}\right)/\mathbb{Z} \cdots \tag{3.76}$$

Example 3.47. Let A, B be groups. Recall that the kernel of $f : A \to B$ is the equalizer of f and $\mathbb{1}$. This is the limit of A, B with morphisms $f, \mathbb{1}$.

Definition 3.18 (Cokernel)**.** An object X of a category $\mathcal{X}$ is the *cokernel* of $A, B \in \operatorname{Obj}(X)$ iff it is the colimit of A, B with respect to the morphisms $f, \mathbb{1}$.

$$\begin{tikzcd}
A \arrow[r, shift left, "f"] \arrow[r, shift right, "\mathbb{1}"'] \arrow[rrd, bend right] & B \arrow[r] \arrow[rd] & Y \\
& & X
\end{tikzcd} \tag{3.77}$$

Remark 3.13. This can also be thought of a general coequalizer of $f, \mathbb{1}$, where the coequalizer is just the equalizer with all arrows reversed.

Definition 3.19. An object $X \in \operatorname{Obj}(\mathcal{C})$ is the *push-out* of A, B with morphisms $f : A \to C$ and $f : B \to C$ iff it is the colimit of A, B with these morphisms.

$$\begin{tikzcd}
& Y & \\
& X \arrow[u, dashed, "\varphi"] & \\
A \arrow[ruu] \arrow[ru, "p_1"] \arrow[rd, "f"] & & B \arrow[luu] \arrow[lu, "p_2"] \arrow[ld, "g"] \\
& C &
\end{tikzcd} \tag{3.78}$$

3.7.2 Exact sequences and direct limits

Example 3.48. We have the general question of when colimits preserve the exactless of a sequence. Consider the following diagram with exact rows:

$$\begin{tikzcd}
& \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & A_i \arrow[r] \arrow[d] & B_i \arrow[r] \arrow[d] & C_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_{i+1} \arrow[r] \arrow[d] & B_{i+1} \arrow[r] \arrow[d] & C_{i+1} \arrow[r] \arrow[d] & 0 \\
& \vdots & \vdots & \vdots &
\end{tikzcd} \tag{3.79}$$

Unfortunately we only have that:

$$\operatorname{colim} A_i \to \operatorname{colim} B_i \to C_i \to 0 \tag{3.80}$$

is right exact but not left exact.

Example 3.49. We now offer an instance where the colimit is not even left exact.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r] \arrow[u, "\times 2"] \arrow[d, "\times 2"] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[u] \arrow[d, "\times 2"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[u] \arrow[d, "\times 2"] & 0 \\
 & \mathbb{Z} \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd} \tag{3.81}$$

The colimit

$$\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \tag{3.82}$$

it not injective.

Remark 3.14. We seek to understand when exact limits are preserved by colimits. To see why, we need to introduce some new concepts.

Definition 3.20 (Directed set)**.** A set S is a directed set iff it is partially ordered and for all $a, b \in S$ we have some $c \in S$ such that $a \leq c$ and $b \leq c$.

Example 3.50. The set $\mathbb{N}$ is directed under the usual ordering $\leq$.

Definition 3.21 (Direct Limit)**.** A colimit is a directed limit iff it is the colimit of a family indexed by a directed set.

Theorem 3.6. *Direct limits preserve exact sequences.*

Proof. Let S be a directed set. Take the colimit of a family of objects indexed by S. In particular we have modules A_i for $i \in S$ with $A_i \to A_j$ when $i \leq j$. Every element of the colimit is represented by some $a \in A_i$ for some i. To see this, consider that any element of the colimit is represented by some sum of elements $a_k \in A_j$ for various $j \in S$. This means we can pick c greater than or equal to all of these values of j and just sum the images of a_j in A_c.

Now let $0 \longrightarrow A_i \longrightarrow B_i \longrightarrow C_i \longrightarrow 0$ be exact for $i \in S$. Then we want to show that $\operatorname{colim} A_i \to \operatorname{colim} B_i$ is injective. Take any $a \in \operatorname{colim} A_i$. This means a is represented by some $a_i \in A_i$ for some $i \in S$. Now let a_i have image 0 in $\operatorname{colim} B_i$. If b_i is the image of s_i, then $b_i = 0$ in the colimit. So there exists $j \in S$ such that the image of b_i in B_j is zero. Then if a_j is the image of a_i in A_j, we have that a_j has image zero. Now we have that $a_j = 0$, which means $A_j \to B_j = 0$, and so $s_j = 0$ in the colimit. □

3.7.3 Inverse limits, p-adic integers

Example 3.51. Consider $G = \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$. This is the colimit of the family:

$$\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \cdots \tag{3.83}$$

But what is G^*? We get:

$$\operatorname{Hom}\left(\mathbb{Z}/p\mathbb{Z}, S^1\right) \longleftarrow \operatorname{Hom}\left(\mathbb{Z}/p^2\mathbb{Z}, S^1\right) \longleftarrow \operatorname{Hom}\left(\mathbb{Z}/p^3\mathbb{Z}, S^1\right) \longleftarrow \cdots \tag{3.84}$$

Definition 3.22 (Inverse limit)**.** The limit of a family of objects in a category is an *inverse limit* iff it is the limit of a directed family.

Remark 3.15. The dual of a direct limit is the inverse limit of the duals.

Definition 3.23 (p-adic integers)**.** A set $\mathbb{Z}_p$ is the set of p-adic integers iff it is the inverse limit of

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \mathbb{Z}/p^2\mathbb{Z} \longleftarrow \mathbb{Z}/p^3\mathbb{Z} \qquad \cdots \tag{3.85}$$

Remark 3.16. This definition is motivated by example example 3.51 The p-adic integers are essentially numbers written out as sequences of base p expansions going infinitely far to the left.

Example 3.52. For example, for $p = 3$, we might have the sequence

$$(\cdots, 2, 1, 2, 2, 0, 1, 2) \tag{3.86}$$

Addition and multiplication are defined component-wise.

Does taking inverse limits preserve exactness? No. Even if the set is directed.

Example 3.53. Take the following diagram:

$$\begin{tikzcd}
& {} \arrow[d] & {} \arrow[d] & & \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z} \arrow[r] \arrow[d, "\times 3"] & \mathbb{Z}/2\mathbb{Z} & \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "\times 3"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[u] \arrow[d, "\times 2"] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 3"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{3.87}$$

note the rows are exact. The inverse limits yield $0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$, but this is not exact.

Remark 3.17. There is still hope. Taking inverse limits preserves exactness if the A_i satisfy the Mittag-Leffler[3.6] condition. See definition 3.24 and theorem 3.7.

[3.6] Surprisingly enough, this is only one person.

3.8 Snake Lemma

3.8.1 Statement and proof of the lemma

Lemma 3.6 (Snake)**.** *Let the following diagram be commutative and exact:*

$$\begin{tikzcd}
 & A_0 \arrow[r, "i_0"] \arrow[d, "f"] & B_0 \arrow[r, "p_0"] \arrow[d, "g"] & C_0 \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A_1 \arrow[r, "i_1"] & B_1 \arrow[r, "p_1"] & C_1 &
\end{tikzcd} \tag{3.88}$$

The map

$$\delta : \ker(h) \to \operatorname{coker}(f) \tag{3.89}$$

induced by $\delta z'' = \alpha^{-1} \circ g \circ \beta^{-1} z''$ is well defined, and we have an exact sequence

$$\begin{tikzcd}
\ker(f) \arrow[r] & \ker(g) \arrow[r] & \ker(h) \arrow[dll, rounded corners, "\delta"] \\
\operatorname{coker}(f) \arrow[r] & \operatorname{coker}(g) \arrow[r] & \operatorname{coker}(h)
\end{tikzcd} \tag{3.90}$$

In other words, we have the following diagram, which shows how δ somehow "fixes" our diagram.

$$\begin{tikzcd}
 & \ker(f) \arrow[r] \arrow[d] & \ker(g) \arrow[r] \arrow[d] & \ker(h) \arrow[d] \arrow[dddll, rounded corners, "\delta"] & \\
 & A_0 \arrow[r, "i_0"] \arrow[d] & B_0 \arrow[r, "p_0"] \arrow[d] & C_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_1 \arrow[r, "i_1"] \arrow[d] & B_1 \arrow[r, "p_1"] \arrow[d] & C_1 \arrow[d] & \\
 & \operatorname{coker}(f) \arrow[r] & \operatorname{coker}(g) \arrow[r] & \operatorname{coker}(h) &
\end{tikzcd} \tag{3.91}$$

Proof. We first construct the snake homomorphism explicitly. Take some $c \in \ker(h)$. Then we have that $c_0 \in C_0$, so since $B_0 \longrightarrow C_0$ is surjective, we can lift c_0 to an element $b_0 \in B_0$. Then we can take b_0 to $b_1 = g(b_0)$. Now since $c_0 \in \ker(h)$, and the diagram commutes, we have that $p_1(b_1) = 0$. Therefore $b_1 \in \ker(p_1) = \operatorname{im}(i_1)$. Therefore we can lift b_1 to $a_1 \in A_1$. Note that a_1 is uniquely determined by b_0, because i_1 is injective. Now let a_2 be the image of a_1 in *coker* $\{f\}$. Let our δ bring $c \mapsto a_2$.

We now show this construction of δ is in fact well defined. This is not immediate because we made a choice of b_0. Consider some other choice $\tilde{b}_0$. Then let $\tilde{a}_1$ be the corresponding element of A_1. Note $p_0\left(b_0 - \tilde{b}_0\right) = 0$, meaning there is some $\tilde{a}_0 \in A_0$ such that $\alpha(\tilde{a}_0) = b_0 - \tilde{b}_0$. Again since the diagram commutes, we have that

$$i_1(f(\tilde{a}_0)) = g\left(b_0 - \tilde{b}_0\right) \tag{3.92}$$

Then since f is injective, and

$$i_1\left(a_1 - \tilde{a}_1\right) = g\left(b_0 - \tilde{b}_0\right) \tag{3.93}$$

we know that $a_1 - \tilde{a}_1 = f\left(\tilde{a}_0\right)$ so $a_1, \tilde{a}_1$ share an image in $\operatorname{coker}(f) = A_1/\operatorname{im}(f)$.

Now we show that the snake sequence is exact. The hard part is showing this for δ. Let us show the exactness at $\operatorname{coker}(f)$. Let $a_2 \in \operatorname{coker}(f)$ such that its image in $\operatorname{coker}(g)$ is zero. Then we can lift a_2 to some $a_1 \in A_1$. Now let $b_1 = i_1(a_1)$. Notice b_1 maps to zero in $\operatorname{coker}(g)$ by the definition of a_2 and since the diagram commutes. Then we can lift it to some $b_0 \in B_0$. Then let $c_0 = p_0(b_0)$ so we have that $h(c_0) = 0$ since

$$g\left(b_0\right) = b_1 \in \operatorname{im}\left(i_1\right) = \ker\left(p_1\right) \tag{3.94}$$

so $c \in \ker(f)$ and $\gamma(c) = a_2$ as desired. The similar proof for $\ker(f)$ is left as an exercise. □

Example 3.54. Taking $A_0 = B_0 = A_1 = B_1 = \mathbb{Z}$ and $C_0 = C_1 = \mathbb{Z}/2\mathbb{Z}$ gives the following diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker(f) \arrow[r] \arrow[d] & \ker(g) \arrow[r] \arrow[d] & \ker(h) \arrow[d] & \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d, "f"', "\times 2"] & \mathbb{Z} \arrow[r] \arrow[d, "g"', "\times 2"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, "h"', "\times 2"] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r] \arrow[d, "\times 2"] & \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & \operatorname{coker}(f) \arrow[r, "\times 2"] \arrow[d] & \operatorname{coker}(g) \arrow[r] \arrow[d] & \operatorname{coker}(h) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{3.95}$$

Then we have that

$$\begin{aligned}
\ker(d') &= \ker(d) = 0 \qquad \ker(d'') = \mathbb{Z}/2\mathbb{Z} && (3.96)\\
\operatorname{coker}(d') &= \operatorname{coker}(d) = \operatorname{coker}(d'') = \mathbb{Z}/2\mathbb{Z} && (3.97)
\end{aligned}$$

Then we have that

$$\ker(d) \longrightarrow \ker(d'') \tag{3.98}$$

is not surjective, and

$$\operatorname{coker}(d') \longrightarrow \operatorname{coker}(d) \tag{3.99}$$

is not injective. The snake lemma somehow identifies these problems as the "same."

3.8.2 Tor

Example 3.55. Let M be a module. Recall that if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{3.100}$$

is exact, then we have that:

$$A \otimes M \longrightarrow B \otimes M \longrightarrow C \otimes M \longrightarrow 0 \tag{3.101}$$

is exact. It is however the case, that our map $A \otimes M \longrightarrow B \otimes M$ is not injective. We now find the kernel of this map. Choose free modules $\{F_i\}, \{H_i\}$ such that

$$0 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0 \qquad 0 \longrightarrow H_1 \longrightarrow H_0 \longrightarrow C \longrightarrow 0 \tag{3.102}$$

are both exact. Then we can extend the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & F_1 \arrow[r] \arrow[d, "f"] & F_1 + H_1 \arrow[r] \arrow[d, "g"] & H_1 \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & F_0 \arrow[r, "\times 2"] \arrow[d] & F_0 + H_0 \arrow[r] \arrow[d] & H_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd} \tag{3.103}$$

Take the tensor product of every row with M, and put in the kernels, to get the diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker(f) \arrow[r] \arrow[d] & \ker(g) \arrow[r] \arrow[d] & \ker(h) \arrow[d] & \\
0 \arrow[r] & F_1 \otimes M \arrow[r] \arrow[d, "f"] & (F_1 \otimes M) + (H_1 \otimes M) \arrow[r] \arrow[d, "g"] & H_1 \otimes M \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & F_0 \otimes M \arrow[r] \arrow[d] & (F_0 \otimes M) + (H_0 \otimes M) \arrow[r] \arrow[d] & H_0 \otimes M \arrow[r] \arrow[d] & 0 \\
 & A \otimes M \arrow[r] \arrow[d] & B \otimes M \arrow[r] \arrow[d] & C \otimes M \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{3.104}$$

Since the last nonzero row is the row of cokernels of the maps f, g, h. This means we can apply the snake lemma to get that:

$$\begin{tikzcd}
0 \arrow[r] & \ker(f) \arrow[r] & \ker(g) \arrow[r] & \ker(h) \arrow[dlll, rounded corners] \\
A \otimes M \arrow[r] & B \otimes M \arrow[r] & C \otimes M \arrow[r, "\delta"] & 0
\end{tikzcd} \tag{3.105}$$

is an exact sequence. We call these:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Tor}(A,M) \arrow[r] & \operatorname{Tor}(B,M) \arrow[r] & \operatorname{Tor}(C,M) \arrow[dll, rounded corners] & \\
& A \otimes M \arrow[r] & B \otimes M \arrow[r] & C \otimes M \arrow[r, "\delta"] & 0
\end{tikzcd} \tag{3.106}$$

Is $\operatorname{Tor}(A,M)$ well defined? This is not immediate because it might depend on the choice of $0 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0$ It is however well defined.

Example 3.56. Let's calculate $\operatorname{Tor}(M,N)$ for some finitely generated abelian groups M,N. First we have

$$\operatorname{Tor}(M_1 \oplus M_2, N) \cong \operatorname{Tor}(M_1,N) \oplus \operatorname{Tor}(M_2,N) \tag{3.107}$$

This means we only need to consider M,N as cyclic. If we have $M,N=\mathbb{Z}$, take the resolution $0 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$. If $M=\mathbb{Z}$ and $N=\mathbb{Z}/n\mathbb{Z}$. Then we have:

$$\begin{tikzcd}
0 \arrow[r] & F_1 \arrow[r] & F_0 \arrow[r] & M \arrow[r] & 0 \\
0 \arrow[r] & 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{3.108}$$

Therefore we have that $\operatorname{Tor}(\mathbb{Z},\mathbb{Z}/n\mathbb{Z})=0$.

If $M=\mathbb{Z}/m\mathbb{Z}$ and $N=\mathbb{Z}/n\mathbb{Z}$, then we have

$$\begin{tikzcd}
0 \arrow[r] & F_1 \arrow[r] & F_0 \arrow[r] & M \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\times m"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/m\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r, "\times m"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \cdots \arrow[r] & 0
\end{tikzcd} \tag{3.109}$$

so we also have

$$\operatorname{Tor}(\mathbb{Z}/m\mathbb{Z},\mathbb{Z}/n\mathbb{Z}) = \ker\left(\ \mathbb{Z}/n\mathbb{Z} \overset{\times m}{\longrightarrow} \mathbb{Z}/n\mathbb{Z}\ \right) = \mathbb{Z}/\left(m,n\right)\mathbb{Z} \tag{3.110}$$

This shows us that $\operatorname{Tor}(M,N)$ depends only on the torsion subgroups of M,N. In fact, if M,N are finite, $M \otimes N \cong \operatorname{Tor}(M,N)$.

Warning 3.3. This isomorphism is not natural.

Example 3.57. We now consider a historical example from algebraic topology. This is where Tor originated.

The universal coefficient theorem states that:

$$H_i(M,G) = \left(H_i(M,\mathbb{Z}) \otimes G\right) \oplus \operatorname{Tor}\left(H_{i-1}(M,\mathbb{Z}),G\right) \tag{3.111}$$

where $H_i(M,G)$ is the homology of the manifold M with coefficients in G.

Example 3.58. We now consider a specific case of example example 3.57. Let $M = P^2$ be the 2-dimensional projective space. This is S^2 where we identify opposite points. Suppose we know that

$$H_0(M,\mathbb{Z}) = \mathbb{Z} \qquad H_1(M,\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \qquad H_i(M,\mathbb{Z}) = 0 \tag{3.112}$$

for $i > 1$. Then we have that:

$$\begin{aligned} H_0(M,\mathbb{Z}/2\mathbb{Z}) &= H_0(M,\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} && (3.113)\\ H_1(M,\mathbb{Z}/2\mathbb{Z}) &= H_1(M,\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} \oplus \operatorname{Tor}(H_0(M,\mathbb{Z}),\mathbb{Z}/2\mathbb{Z}) && (3.114)\\ H_2(M,\mathbb{Z}/2\mathbb{Z}) &= H_2(M,\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} \oplus \operatorname{Tor}(H_1(M,\mathbb{Z}),\mathbb{Z}/2\mathbb{Z}) && (3.115) \end{aligned}$$

which allows us to compute the homology group $H_2(M,\mathbb{Z}/2\mathbb{Z})$.[3.7]

3.8.3 Mittag-Leffler condition

Definition 3.24. Consider some sequence:

$$\cdots \longrightarrow A_3 \longrightarrow A_2 \longrightarrow A_1 \longrightarrow A_0 \tag{3.116}$$

The *Mittag-Leffler condition* is that the sequence of images stabilizes for all A_n. In particular, for each $n \in \mathbb{N}$ there exists some $i \geq n$ such that $\operatorname{im}(A_i) = \operatorname{im}(A_{i+1}) = \cdots$.

Remark 3.18. The general idea of this condition is that eventually, the sequence stabilizes and stops getting smaller.

Example 3.59. The Mittag-Leffler condition holds if all A_i are finite.

Theorem 3.7. *Consider the following diagram:*

$$\begin{tikzcd} & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\ 0 \arrow[r] & A_{i+1} \arrow[r] \arrow[d] & B_{i+1} \arrow[r] \arrow[d] & C_{i+1} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A_i \arrow[r] \arrow[d] & B_i \arrow[r] \arrow[d] & C_i \arrow[r] \arrow[d] & 0 \\ & \vdots & \vdots & \vdots & \end{tikzcd} \tag{3.117}$$

If the Mittag-Leffler condition is satisfied, then

$$0 \longrightarrow \lim A_i \longrightarrow \lim B_i \longrightarrow \lim C_i \longrightarrow 0 \tag{3.118}$$

is also exact.

[3.7] In the first edition of Lang's Algebra [5] there was an exercise: "Take any book on homological algebra, and prove all the theorems without looking at the proofs given in that book." This was removed in later editions.

Proof. There are two cases.

1. First suppose that every map $A_{i+1} \to A$ is onto. This satisfies the ML condition. We want to show that $\lim B_i \to \lim C_i$ is onto. Pick any element of $\lim C_i$. This can be written $(c_0, c_1, \cdots)$ for $c_i \in C_i$ where c_i is the image of c_{i+1}. We can lift the c_i to b_i. We can then as if b_i is the image of b_{i+1}? Pick some $b_0 \in B_0$, and choose some $b_1 \in B_1$. Then we have that

$$\operatorname{im}(b_1) - b_0 \in \ker(B_0 \to B_0) = \operatorname{im}(A_0 \to B_0) \tag{3.119}$$

so we let $a_0 \in A_0$ be its pre-image. Then we can list a_0 to $a_1 \in A_1$. Now replace b_1 by $b_1 + \operatorname{im}(a_1)$. Repeat this process for $b_2, b_3, \cdots$ so we get that b_i maps to c_i and b_{i-1}.

2. Suppose for each i, we can find some j so that $A_j \to A_i$ is 0. This is the extreme opposite condition to case 1. Then the ML condition holds. We want to show that $\lim B_i \to \lim C_i$ is onto. Pick A_{i_1} such that $A_{i_1} \to A_{i_0}$ is zero. Do the same over and over to get

$$\cdots \to \qquad A_{i_2} \longrightarrow A_{i_1} \longrightarrow A_{i_0} \tag{3.120}$$

Take the inverse limit over $B_0, B_{i_1}, B_{i_2} \cdots$. Then we can assume all maps $A_{i+1} \to A_i$ are zero. Pick $(c_0, c_1, c_2, \cdots)$ and pick b_i which gets mapped to c_i. We might wonder if $\operatorname{im}(b_i) = b_{i-1}$. We do know that $\operatorname{im}(b_2) = b_1$ since $\operatorname{im}(b_2) - b_1$ is in the image of A_1 which is 0 in A_0. Therefore the sequence of images of b_i is in $\lim B_i$, and has image $(c_0, c_1, \cdots)$.

Now we combine the previous two cases. Suppose A_i satisfies the ML condition. Put

$$X_i = \bigcap_{j \geq i} \operatorname{im}(A_j \to A_i) \tag{3.121}$$

Therefore we have that $X_i \subseteq A_i$ and we have the following exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & X_i \arrow[r] \arrow[d] & A_i \arrow[r] \arrow[d] & A_i/X_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & X_{i-1} \arrow[r] & A_{i-1} \arrow[r] & A_{i-1}X_{i-1} \arrow[r] & 0
\end{tikzcd} \tag{3.122}$$

where the maps between the X_i elements of the sequences are surjective. For each i, we can find a j so that

$$\operatorname{im}(A_j/X_i \to A_i/X_i) = 0 \tag{3.123}$$

Now we can use the snake lemma. Recall that $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ implies

$$A \otimes M \longrightarrow B \otimes M \longrightarrow C \otimes M \longrightarrow 0 \tag{3.124}$$

is exact and

$$\begin{tikzcd}
\operatorname{Tor}(A,M) \arrow[r] & \operatorname{Tor}(B,M) \arrow[r] & \operatorname{Tor}(C,M) \arrow[dll, hook] & \\
A \otimes M \arrow[r] & B \otimes M \arrow[r] & B \otimes M \arrow[r] & 0
\end{tikzcd} \tag{3.125}$$

is exact.

Now we can make this same argument since the limit is exact. We do this by flipping all the arrows. We constructed Tor by taking

$$0 \longrightarrow G_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0 \tag{3.126}$$

where this only works when F is free, or projective. So now we flip the arrows by replacing the projective modules by injective modules

$$0 \longrightarrow A \longrightarrow I_0 \longrightarrow I_1 \longrightarrow 0 \tag{3.127}$$

since every module is contained in some injective module.

The analogue of Tor is then revealed to be $\varprojlim (A_1)$. We get a sequence

$$\begin{tikzcd}
0 \arrow[r] & \lim A_i \arrow[r] & \lim B_i \arrow[r] & \lim C_i \arrow[dll, hook] \\
 & \varprojlim A_i \arrow[r] & \varprojlim B_i \arrow[r] & \varprojlim C_i
\end{tikzcd} \tag{3.128}$$

Now we need $\varprojlim A_i = 0$ in order for this to be exact. The proofs above show that this is true as long as either of the special cases hold. So look at $0 \longrightarrow X_i \longrightarrow A_i \longrightarrow A_i/X_i \longrightarrow 0$ and notice that we have:

$$\begin{tikzcd}
0 \arrow[r] & \lim X_i \arrow[r] & \lim A_i \arrow[r] & \lim A_i/X_i \arrow[dll, hook] & \\
 & \varprojlim X_i \arrow[r] & \varprojlim A_i \arrow[r] & \varprojlim A_i/X_i \arrow[r] & 0
\end{tikzcd} \tag{3.129}$$

□

3.9 Finitely generated modules over a PID

Theorem 3.8. *Any finitely generated module of a PID is a sum of cyclic modules of the form R/I.*

sketch. We cheat a bit and just do the case considering Euclidean domains. The proof is therefore the same as the one for $\mathbb{Z}$. If M is a submodule of $\mathbb{Z}^n$ then we have some basis $\{b_i\}_1^n$ of $\mathbb{Z}^n$. Therefore for some $\{d_i\}_1^n$ we have that M is spanned by $\{d_i b_i\}_1^n$. Then the finitely generated module:

$$\mathbb{Z}^n/M = \bigoplus \mathbb{Z}/d_i\mathbb{Z} \tag{3.130}$$

as desired. □

Chapter 4

Polynomials

4.1 Preliminaries

Unless stated otherwise, R will be a commutative ring throughout this chapter. We first state some basic results without proof.

Theorem 4.1. *Let $f, g \in R[x]$ be polynomials with coefficients in R. Let f have leading coefficient 1. There we have polynomials $q(x), r(x) \in R[x]$ such that*

$$g(x) = f(x) q(X) + r(x) \tag{4.1}$$

where $\deg(r) < \deg(f)$.

Corollary 4.1. *Let K be a field. The ring $K[x]$ is a Euclidean domain.*

Proof. We can assume the leading coefficient of any polynomial to be 1, since K is a field. As such, we can apply theorem theorem 4.1. □

Corollary 4.2. *Let K be a field. We then have that $K[x]$ is a principal ideal domain, and unique factorization domain.*

Proof. By corollary corollary 4.1, $K[x]$ is a Euclidean domain. From theorems 2.1 and 2.2 all Euclidean domains are principal ideal domains, and all principal ideal domains are unique factorization domains. □

Example 4.1. How might we find the prime elements of the ring $F_2[x]$ where $F_2 = \mathbb{Z}/2\mathbb{Z}$? Recall the sieve of Eratosthenes. This is a method for finding prime numbers. We first list the numbers ≥ 1, declare the first number prime, and cross off the multiples of it:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, \cdots \tag{4.2}$$

We declare the next number left nor crossed out as prime, and cancel the multiples of this number:

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, \cdots \tag{4.3}$$

and repeat like this. Eventually only the prime numbers will be left. We use this as motivation.

We first list elements of $F_2[x]$ in order of degree:

$$x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, \cdots \tag{4.4}$$

So now cross our multiples of x:

$$\cancel{x}, x+1, \cancel{x^2}, x^2+1, \cancel{x^2+x}, x^2+x+1, \cdots \tag{4.5}$$

Then the next element $x+1$ is prime, so we cross out multiples of this:

$$\cancel{x}, x+1, \cancel{x^2}, x^2+1, \cancel{x^2+x}, \cancel{x^2+x+1}, \cdots \tag{4.6}$$

So we end up with a list of all the prime elements up to degree 4:

$$x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, \cancel{x^4+x^2+1}, x^4+x^3+1, x^4+x^3+x^2+x+1 \tag{4.7}$$

we can continue this process to obtain all prime elements.

Proposition 4.1. *Suppose a polynomial $f \in R[x]$ has a root a, then there exists some $g \in R[x]$ such that*

$$f(x) = g(x)(x-a) \tag{4.8}$$

Proof. Apply the division algorithm to $f(x)$. This gives some g, r such that

$$f(x) = g(x)(x-a) + r(x) \tag{4.9}$$

but then we have $\deg(r) < 1$ which means r is constant. Now taking $x = a$, we have $f(a) = g(a)(a-a) + r = r = 0$ which is zero because a is a root by assumption. □

Corollary 4.3. *Any polynomial $f \in R[x]$ of degree n where R is an integral domain has at most n roots.*

Proof. If we have $\{a_i\}_{i=1}^k$ roots of f, then by proposition proposition 4.1 we have that for some $g(x)$

$$f(x) = (x-a_1)\cdots(x-a_k)\,g(x) \tag{4.10}$$

which means $k \leq n$. If the product is zero, then we must have that some factor $(x-a_i)$ is zero because R is an integral domain. □

Example 4.2. Let $R = \mathbb{Z}/8\mathbb{Z}$. Then R is not an integral domain, so taking $f(x) = x^2 - 1 \in R[x]$ we see that f has roots $1, 3, 5, 7$ which is more than 2. Showing that the assumption that R is an integral domain is necessary in corollary corollary 4.3.

Example 4.3. Let R be the quaternions. Recall the quaternions are noncommutative. Now look at $f(x) = x^2 + 1$. This has roots $\pm i, \pm j, \pm k$ and $ai + bj, ck$ for $a, b, c \in \mathbb{R}$ such that $a^2 + b^2 + c^2 = 1$. This means f has an uncountable number of roots. Again showing that the assumption that R is an integral domain (and hence commutative) is necessary in corollary corollary 4.3.

4.2 Application to fields

Lemma 4.1. *Let G be an abelian group with at most n elements of order n. Then G is cyclic.*

Proof. Recall that for some primes $\{p_i\}$ and $\{n_i\} \subseteqq \mathbb{N}$ we have:

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots \tag{4.11}$$

Now suppose $p_1 = p_2$. Then G has p^2 elements x such that $x^p = 1$, since $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \subseteqq G$. This is impossible, so we can assume the $\{p_i\}$ are distinct. Now we have that G is cyclic by the Chinese remainder theorem ($\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if $\gcd(m,n) = 1$.) □

Proposition 4.2. *Let p be prime. Then the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Since p is prime, $R = \mathbb{Z}/p\mathbb{Z}$ is a field. Therefore any polynomial in $R[x]$ of degree n has $\leq n$ roots. In particular, $x^n - 1$ has at most n roots for any $n \geq 1$. This means G has $\leq n$ elements x such that $x^n = 1$. Then applying lemma lemma 4.1 we are done. □

Example 4.4. Note proposition proposition 4.2 does not apply when p is not prime. For example, consider $(\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$ where these are both cyclic of order 2.

Definition 4.1. An element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a *primitive root* iff it is a generator.

Remark 4.1. We have shown primitive roots always exist when p is prime. It is however hard to actually find primitive roots. Effectively, the only available algorithms are checking the options one by one.

Example 4.5. We want to find the primitive roots of $(\mathbb{Z}/p\mathbb{Z})^\times$ for $p = 23$. We check the elements, $-1, 1, 3, 4, 5$. This shows 5 is the primitive root, because we have

$$5^2, 5^{11} \not\equiv 1 \pmod{23} \tag{4.12}$$

Theorem 4.2. *Let F be a field. Then any finite subgroup of $F^\times$ is cyclic.*

Example 4.6. Take $F = \mathbb{C}$ for example. The subgroup of the 8th roots of unity give a subgroup with generator $\exp(i2\pi/8)$.

Corollary 4.4. *Let F be a finite field. We then have that $F^\times$ is cyclic.*

4.3 Unique factorization in polynomial rings

Remark 4.2. We would like to show that $\mathbb{Z}[x]$ is a UFD. We know that $\mathbb{Z}[x] \subseteq \mathbb{Q}[z]$ and furthermore that $\mathbb{Z}[x]$ is a UFD itself, since $\mathbb{Q}$ is a field. We cannot use our usual methods because $\mathbb{Z}[x]$ is not a PID or a Euclidean domain. This is easily seen by the fact that $(2, x)$ is a non-principal ideal. We instead must use the fact that $\mathbb{Q}[x]$ is a UFD.

Definition 4.2 (Content)**.** Let $f \in \mathbb{Q}[x]$ and $\partial \in \mathbb{Z}$ be prime. Write:

$$f(x) = x^n a_n + \cdots + a_0 \tag{4.13}$$

Then we have

$$a_n = p^{m_n} b_n \qquad a_{n-1} = p^{m_{n-1}} b_{n-1} \qquad \cdots \tag{4.14}$$

where $\{m_i\}_{i=1}^n \subseteq \mathbb{Z}$ and the $\{b_i\}_{i=1}^n$ have no factors of p in the numerator or denominator. Then the number $\mathrm{c}(f)$ is the content of f iff

$$\mathrm{c}(F) = p^{\min(m_i)} b \tag{4.15}$$

where b is some number with no factors of p.

Example 4.7. If $f = (2/3)x^2 + 4$ then we have $\mathrm{c}(F) = 2/3$.

Lemma 4.2. *Let $f, g \in \mathbb{Z}[x]$ then we have*

$$\mathrm{c}(fg) = \mathrm{c}(f)\,\mathrm{c}(g) \tag{4.16}$$

Proof. WLOG we may assume that $\mathrm{c}(f) = \mathrm{c}(g) = 1$, for if not, we may just multiply by some constant to make it so. Therefore it is sufficient to show that $\mathrm{c}(fg) = 1$. First note that since f has integer coefficients, $\mathrm{c}(f) \in \mathbb{Z}$. Now let p be any prime. We show that p does not divide $\mathrm{c}(fg)$.

Since we have that the $\mathrm{c}(f) = \mathrm{c}(g) = 1$, it cannot be possible for p to divide all of the coefficients of f or g by definition of the content of a polynomial. As such, if we write

$$f(x) = a_n x^n + \cdots + a_i x^i + \cdots + a_0 \qquad g(x) = b_n x^n + \cdots + b_i x^i + \cdots + b_0 \tag{4.17}$$

then we have that the coefficient of the x^{i+j} term of fg, is

$$a_0 b_{i+j} + a_1 b_{i+j-1} \cdots a_i b_j + a_{i+j-1} b_1 + a_{i+j} b_0 \tag{4.18}$$

Notice each of these terms is divisible by p, except for the $a_a b_j$ term. This means the entire coefficient of $x_i y_j$ is not divisible by p. Since p was arbitrary we are done. □

Lemma 4.3. *The only irreducibles of $\mathbb{Z}[x]$ are the prime integers and polynomials f such that $\mathrm{c}(f) = 1$. Furthermore, every element of $\mathbb{Z}[x]$ is a product of irreducibles.*

Proposition 4.3. *$\mathbb{Z}[x]$ is a unique factorization domain.*

Proof. We only sketch this. The main point here is to show that irreducible elements are prime. Recall that this means that $f \neq gh$ for $\deg(g), \deg(h) < \deg(f)$. Prime elements are such that if $f|gh$ then $f|g$ or $f|h$. Therefore by lemmas lemma 4.2,lemma 4.3 we know that if $\deg(f) = 0$ then $f = p$ is prime in $\mathbb{Z}$. If $f|gh$, then $p|\,\mathrm{c}(gh)$ so either $\mathrm{c}(g)$ of $\mathrm{c}(h)$ is divisible by p, and therefore $p|gh$. The case of $\deg(f) > 0$ is left as an exercise. □

Theorem 4.3. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Perform the same proof as in proposition 4.3 with some minor changes. Here we only know $\mathrm{c}(f)$ up to a unit. Now irreducibles of $\mathbb{R}[x]$ are either irreducibles of R, or irreducibles of $K[x]$ with content of 1 where K is the quotient field of R. □

Corollary 4.5. *$\mathbb{Z}[x_1, \cdots, x_n]$ is a UFD.*

Proof. Induction on number of variables. □

Remark 4.3. In fact, we even have $\mathbb{Z}[x_1, \cdots]$ of infinitely many variables is a field, but we do not prove this.

Corollary 4.6. *If K is a field, $K[x_1, x_2, \cdots, x_n]$ is a UFD.*

Proof. Induction on number of variables. □

4.4 Irreducibility

4.4.1 Basic algorithms

Example 4.8. We now outline an algorithm due to Kronecker: Let $f = gh$. We can assume $g, h \in \mathbb{Z}[x]$. Then $f(n) = g(n)h(n)$ for all $n \in \mathbb{Z}$. Therefore setting $m = \deg(f)$ we can factor

$$f(0), f(1), \cdots, f(m) \tag{4.19}$$

Then we have that $g(0)|f(0)$ of $g(1)|f(1)$ etc. which means we only have a finite number of possibilities for $g(0), \cdots, g(m)$. But we also know that $\deg(g) \le m$ so g is determined by $g(0), \cdots, g(m)$.

Remark 4.4. Kronecker's algorithm is rather slow, so we investigate alternatives.

Example 4.9. The LLL[4.1] algorithm is reasonably fast, but there is a cost to this, since it is not entirely precise. First we take

$$f = af_1f_2\cdots f_n \tag{4.20}$$

where $a \in \mathbb{Z}$, and f_i is irreducible with degree > 0 for all i. This can be done in polynomial time, but to find this a, the algorithm must factor an integer, which cannot be done in polynomial time.

Proposition 4.4. *Another way to test for reducibility is to factorize modulo p. So if we have $f(x) = g(x)h(x)$ we take*

$$f(x) = f(x)h(x) \pmod p \tag{4.21}$$

for some prime p.

[4.1] This stands for Lenstra, Lenstra, Lovasz

Example 4.10. Consider the following polynomial:

$$f = 9x^4 + 6x^3 + 26x^2 + 13x + 3 \tag{4.22}$$

We desire to find out whether this polynomial is reducible or not. It is in fact, since

$$f \equiv x^4 + x + 1 \pmod{2} \tag{4.23}$$

and we already saw this was irreducible.

Example 4.11. Consider the following polynomial:

$$f = x^4 - x^2 + 3x + 1 \tag{4.24}$$

We desire to find out whether or not this polynomial is reducible. We first consider it modulo 2.

$$x^4 + x^2 + x + 1 = (x + 1)\left(x^3 + x^2 + 1\right) \equiv f mod p 2 \tag{4.25}$$

which we know are both irreducible from before. we now consider modulo 3:

$$x^4 - x^1 + 1 = \left(x^2 + 1\right)^2 \equiv f \pmod{3} \tag{4.26}$$

which is also irreducible. Combining these results gives that from the first one, if there is a prime factorization, it must be into a degree 1 and 3 polynomial, whereas the second expression tells us two degree 2 polynomials, and therefore there cannot be a legitimate prime factorization.

4.4.2 Eisenstein's Criterion

Theorem 4.4 (Eisenstein's criterion)**.** *Let f have the following properties:*

1. *The leading coefficient is* 1.
2. *All other coefficients are divisible by p.*
3. *The constant term is not divisible by p^2.*

then f is irreducible.

Proof. See [5]. □

Example 4.12. Consider the polynomial $f = x^5 - 4x + 2$. This is irreducible by theorem theorem 4.4, Eisenstein's criterion.

Example 4.13. Consider the pth roots of unity. These are in fact the roots of the polynomial

$$x^p - 1 = (x - 1)\left(x^{p-1} + x^{p-2} + \cdots + x + 1\right) \tag{4.27}$$

now we want to show that the second term is irreducible. But we can't use Eisenstein's criterion on it in its current state. Luckily we have a trick to get the proper multiples: we can take $z = x - 1$ as our variable, to get:

$$\begin{aligned} x^{p-1} + \cdots + x + 1 &= \frac{x^p - 1}{x - 1} = \frac{(z+1)^p - 1}{z} \quad (4.28) \\ &= \frac{1}{z}\left(z^p + pz^{p-1} + \frac{p(p-1)}{2} z^{p-1} + \cdots + pz\right) \quad (4.29) \\ &= z^{p-1} + pz^{p-2} + \cdots + p \quad (4.30) \end{aligned}$$

as desired. This seems like a mysterious trick, why does it work? As it turns out, this is a consequence of p being *totally ramified*[4.2] in the ring $\mathbb{Z}[\zeta]$ where $\zeta^p = 1$. In particular, let $\zeta = e^{i2\pi/p}$. We have that p factorizes in $\mathbb{Z}[\zeta]$[4.3] as $(1-\zeta)^{p-1} u$ for some unit u. Notice this polynomial has roots:

$$\zeta, \zeta^2, \cdots, \zeta^{p-1} \quad (4.31)$$

which are the pth roots of unity. Additionally,

$$\left(\zeta^k - 1\right) = (\zeta - 1)\left(\zeta^{k-1} + \cdots + 1\right) \quad (4.32)$$

Conversely, $\zeta - 1$ is divisible by $\zeta^k - 1$ so ζ^k also has a root of one.

4.4.3 Rational roots

Proposition 4.5. *Consider the polynomial:*

$$f = x^n + a_{n-1}x^{n-1} \cdots + a_0 \quad (4.33)$$

Then the only linear factors of f are of the form $x - b$ for $b|a_0$. If the leading coefficient is not 1, then our roots can only be $\alpha = b/d$ where $b|a_0$ and $d|a_n$.

Proof. To see this consider that

$$(cx + b)(\cdots) = x^n + \cdots + a_0 \quad (4.34)$$

so we have that

$$1 = c \times \bullet \qquad a_0 = b \times \bullet \quad (4.35)$$

as desired. □

Lemma 4.4. *Every polynomial with no linear factors of degree ≤ 3 is irreducible.*

Proof. This is fine to check at these low degrees, but for ≥ 4, this is a difficult process. □

[4.2] This is an important topic in algebraic number theory. For more, see [4].

[4.3] This is called a *cyclotomic ring*.

Example 4.14. It is not possible to trisect an angle of 120° with only a compass and ruler. To illustrate this we will show that we cannot construct $2\cos(40°) = 2\cos(2\pi/9)$. We will use the following fact without proof:

Claim 4.1. *Any number than can be "constructed" cannot satisfy an irreducible polynomial of degree n, unless n is a power of 2.*

We will show that $\cos(2\pi/9)$ satisfies an irreducible polynomial in $\mathbb{Z}[x]$ of degree 3.

Consider $z = \exp(2\pi i/9)$. Then we have that $\cos(2\pi/9) = z + z^{-1}$. Now we take the polynomial:

$$f = 0 = z^9 - 1 = \left(z^3 - 1\right)\left(z^6 + z^3 + 1\right) \tag{4.36}$$

which means $z^6 + z^3 + 1 = 0$ and therefore $z^3 + 1 + z^{-3} = 0$ so taking $c = z + z^{-1}$ we have that $c^3 - 3c + 1 = 0$. To see that this polynomial is irreducible, it is sufficient to check that it has no linear factors over $\mathbb{Q}$. By lemma lemma 4.4 it is enough to check that the factors of the constant term are not roots.

Example 4.15. Consider the following polynomials:

$$f = x^{100} + 2g = x^{100} + 3h = x^{100} + 4 \tag{4.37}$$

f and g are both irreducible, but h is a counterexample to the intuition that polynomials of this form are irreducible since:

$$g = \left(x^{50} + 2x^{25} + 2\right)\left(x^{50} - 2x^{25} + 2\right) \tag{4.38}$$

4.5 Noetherian rings and polynomials

4.5.1 Noether's theorem

Definition 4.3 (Noetherian)**.** A ring is *Noetherian* iff all ideals of the ring are finitely generated.

Remark 4.5. Emmy Noether circumvented the complicated techniques of the day by introducing this simple classification.

Theorem 4.5. *Let R be a ring. TFAE:*

1. *R is Noetherian*

2. *Every non-empty set of ideals of R has a maximal element.*

3. *Every strictly increasing chain of ideals is finite.*

Proof. (2) $\iff$ (3): First note that Zorn's lemma 2.2 gives us (3) $\implies$ (2) for free. To show the other direction we assume there is some infinite strictly increasing chain of ideals. Then the set of all such ideals cannot have a maximal element. Note this part of the proof does not use that R is a ring, it only uses the fact that ideals of R form partially ordered sets. As such, this result holds for all partially ordered sets.

(1) $\implies$ (3): Suppose that we have $I_1 \subseteq I_2 \subseteq \cdots$ an increasing chain of ideals. Then define $I = \cup_i I_i$. Then we know I is an ideal itself, and by condition (1) we have that $I = (x_1, \cdots, x_n)$ so x_i is in some I_m for all i. Therefore $I_m = I_{m+1} = \cdots$ as desired.

(3) $\implies$ (1): Let I be an ideal. We WTS that I is finitely generated. Take some $x_1 \in I$. Then if $I = (x_1)$ we are done. If not then we take some $x_2 \in I$ such that $x_2 \neq x_1$. If $I = (x_1, x_2)$ then we are done. If not, we continue leading to a chain:

$$(x_1) \subseteq (x_1, x_2) \subseteq \cdots \tag{4.39}$$

which must stop after a finite number of elements from condition (3). As such, $I = (x_1, \cdots, x_n)$ for some n as desired. □

Example 4.16. Let $R = K[x_1, x_2, \cdots]$. Then we have that

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots \tag{4.40}$$

so R cannot be Noetherian.

Example 4.17. Consider $R = \mathbb{Z}$. Then we have the infinite strictly decreasing chain of ideals

$$(2) \subset (4) \subset (8) \subset (16) \subset \cdots \tag{4.41}$$

This feature (or the lack thereof) is given a general description in the definition below:

Definition 4.4 (Artinian)**.** A ring R is called *Artinian* iff every strictly ascending sequence of ideals of R eventually terminates.

Proposition 4.6. *All Artinian rings are Noetherian.*

Theorem 4.6 (Noether)**.** *If R is a Noetherian ring, so is $R[x]$.*

Proof. Let I be an ideal of $R[x]$. Then consider the chain of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots$ where I_k is the set of leading coefficients of polynomials in I of non-positive degree. We know R is Noetherian, so there is some m such for all $s \geq m$, $I_s = I_m$. Now pick the set of polynomials of degree 0 such that the leading coefficients generate I_0. We know I_0 is finitely generated because I is Noetherian. Now do this for polynomials of degree $1, 2, \cdots, m$ where we stop because at this point each additional degree will result in the same ideal, since the chain stabilizes here. We leave it as an exercise to show that these finite sets generate I. □

4.5.2 Hilbert's Theorem

Theorem 4.7. *If I is an ideal of the ring $K[x_1, \cdots, x_n]$ then I is finitely generated.*

Proof. Use induction on the number of variables in Noether's theorem. □

Example 4.18. Consider the ring $R = K[x]$. Recall that all the ideals of R are generated by one element from corollary 4.1 and corollary 4.2. We see now that this is not true in general for $K[x, y]$. Look at the ideal $\left(x^3, x^2y, xy^2, y^2\right)$. This ideal needs at least 4 generators, since no element in this set generates more than 1 of these 4 elements. In general, ideals of $K[x_1, \cdots, x_n]$ need not be generated by n elements.

Remark 4.6. These ideals can be visualized by lining up the elements in a grid, and circling the included elements.

Example 4.19. This is not necessarily the case for infinitely many variables. Consider $K[x_1, x_2, \cdots]$. This has the ideal $(x_1, x_2, \cdots)$ which cannot be finitely generated.

Example 4.20. Look at the ideal (x) of the ring $K[x, y]$. We know (x) is a ring (without an identity element) and is not finitely generated as a ring. For example, we might generate this with $\left\{x, xy, xy^2, \cdots\right\}$

Warning 4.1. This brings to our attention a general difference between being finitely generated as an ideal of a ring, and being finitely generated as a ring.

4.6 Invariants and symmetric functions

Example 4.21. Let G be a group acting on a vector space V. Let V have basis $\{x_i\}_{i=1}^n$. Then for any $g \in G$ we have:

$$g \cdot x_1 = g_{1,1}x_1 + g_{1,2}x_2 + \cdots + g_{1,n}x_n \tag{4.42}$$

Now G can also act on polynomials in $\{x_i\}$ by the action given by:

$$g \cdot (p + q) = g \cdot p + g \cdot q \qquad\qquad g \cdot (pq) = (g \cdot p)(g \cdot q) \tag{4.43}$$

Definition 4.5 (Ring of invariants)**.** The *ring of invariants* is the set of polynomials fixed by G. That is, the polynomials p such that for all $g \in G$, $g \cdot p = p$.

Remark 4.7. We might wonder now if we can find a finite collection of particular invariants such that all invariants are polynomials in them with coefficients in K. Hilbert showed this is often true, and about 50 years later, Nagata found a counterexample to show it is not always true.

Definition 4.6 (Symmetric function)**.** Let V be a vector space with basis $\{x_i\}_{i=1}^n$. Let G be the symmetric group on the basis of V. Then the ring of *symmetric functions* is the ring of invariant polynomials.

Remark 4.8. Symmetric functions are deeply related to combinatorics.

Example 4.22. We consider some examples of symmetric functions:

$$x_1 + x_2 + \cdots + x_n \tag{4.44}$$

$$x_1 x_2 \cdots x_n \tag{4.45}$$

$$x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \tag{4.46}$$

$$x_1x_2x_3 + x_1x_2x_4 + \cdots + x_1x_3x_4 + \cdots \tag{4.47}$$

Now consider

$$(x - x_1) \cdots (x - x_n) = x^n - \sum_i x_i \, x^{n-1} + \sum_{i<j} x_i x_j \, x^{n-2} + \cdots \pm \prod x_i \tag{4.48}$$

The coefficients of this polynomial are the *elementary symmetric functions.*

Theorem 4.8. *All symmetric functions are a polynomial in elementary symmetric functions.*

Proof. We prove this with an algorithm. The key idea is to order the monomials in the proper way.[4.4] We order them as follows:

$$x_1^{n_1} x_2^{n_2} \cdots \geq x_1^{m_1} x_2^{m_2} \cdots \iff (n_1, n_2, \cdots) \geq (m_1, m_2, \cdots) \tag{4.49}$$

with a lexicographic order.

Let p be a symmetric polynomial. Consider the biggest monomial in p. We write this

$$x_1^{n_1} x_2^{n_2} \cdots \tag{4.50}$$

Subtract

$$(x_1 + \cdots + x_n)^{n_1 - n_2} (x_1 x_2 + \cdots)^{n_2 - n_3} \tag{4.51}$$

The key point here is that $n_1 \geq n_2 \cdots$ since f is symmetric. Suppose f contains (say) $x_1^2 x_2^2$ then since f is symmetric, it also contains $x_3^3 x_2^2$. We repeat this process until we get 0, since we know we don't have an infinite sequence of strictly decreasing monomials. We leave the rest of the proof as an exercise. □

Definition 4.7. The *logarithmic derivative* of a function f is

$$\frac{d}{dx} (\log (f)) = \frac{f'}{f} \tag{4.52}$$

Proposition 4.7. *For two functions f, g we have*

$$(\log (fg))' = (\log (f) + \log (g))' = (\log (f))' + (\log (g))' \tag{4.53}$$

Example 4.23. We consider applications to Newton's identities. We want to find an expression for (say) $\sum_i x_i^4$. To find this look at

$$f(x) = (x - x_1) \cdots (x - x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \cdots \tag{4.54}$$

[4.4] This ordering is important in the study of Gröbner bases.

where e_i are the elementary symmetric functions. Now we want sums of powers of x_i, so we take the logarithmic derivative of this. This gives:

$$(\log(x-x_1))' = \frac{1}{x-x_1} = \frac{1}{x} + \frac{x_1}{x^2} + \frac{x_1^2}{x^3} + \cdots \tag{4.55}$$

so

$$\begin{aligned}
(\log(f))' &= \frac{n}{x} + \frac{(x_1+x_2+\cdots)}{x_2} + \cdots & (4.56)\\
&= \frac{p_0}{x} + \frac{p_1}{x^2} + \frac{p_2}{x^3} + \cdots & (4.57)\\
&= \frac{f'}{f} & (4.58)
\end{aligned}$$

where $p_m := \sum_i x_i^m$ and $p_0 = n$. This means

$$\begin{aligned}
f\left(\sum \frac{p_m}{x^{m+1}}\right) &= f' & (4.59)\\
\left(x^n - e_1x^{n-1} + \cdots\right) &= nx^{n-1} - (n-1)\,e_1x^{n-2} + \cdots & (4.60)
\end{aligned}$$

so

$$\begin{aligned}
p_0 &= n & (4.61)\\
p_1 - e_1p_0 &= -(n-1)\,e_1 & (4.62)\\
p_2 - e_1p_1 + e_2p_0 &= (n-2)\,e_2 & (4.63)
\end{aligned}$$

which gives us values of p_0, p_1, p_2 as desired.

Example 4.24. Let α, β, γ be roots of z^3+z+1. We want to find $\alpha^5+\beta^5+\gamma^5$. We know that

$$\begin{aligned}
p_0 &= 3 \qquad p_1 = 0 \qquad p_2 + p_0 = 1 & (4.64)\\
p_2 &= -1 \qquad p_3 = -3 \qquad p_4 = 2 \qquad p_5 + p_3 + p_2 = 0 & (4.65)
\end{aligned}$$

which give the coefficients of the polynomial.

4.6.1 The discriminant

Definition 4.8. Let f be a polynomial in $x_1, \cdots, x_n$. f is antisymmetric iff it changes sign under elements $\sigma \notin A_n$.

Proposition 4.8. *Let f be invariant under A_n. We then have some symmetric g, and some antisymmetric h such that $f = g + h$.*

Proof. We define:

$$g := \frac{f+\sigma f}{2} \qquad h := \frac{f-\sigma f}{2} \tag{4.66}$$

The rest of the proof is left as an exercise. □

Definition 4.9 (Discriminant)**.** Let

$$\Delta \coloneqq \prod_{i<j} (x_i - x_j) \tag{4.67}$$

The *discriminant*[4.5] of a polynomial $f(x) = a_n x^n + \cdots + x_0$ is $a_n^{2n-2}\Delta^2$.

Claim 4.1. The discriminant vanishes iff f has multiple roots.

Proposition 4.9. *Invariant functions of A_n are generated by the symmetric functions $e_1, \cdots, e_n$ and Δ. We can also see that Δ^2 itself is symmetric, so Δ^2 is some polynomial in $e_1, \cdots, e_n$. This is referred to as syzygy.*[4.6]

Remark 4.9. An antisymmetric polynomial h (as in (4.66)) changes sign if we switch x_i, x_j which motivates the previous definition of Δ.

Proposition 4.10. *Let f be a polynomial. f has multiple roots iff f, f' have a common factor.*

Proof. If $f = (x - x_1)^2 \cdots$, we have

$$f' = 2(x - x_2) \cdots + (x - x_1)^2 \tag{4.68}$$

meaning they share a factor of $(x - x_1)$. The converse is left as an exercise. □

4.6.2 Conditions for common factors

Example 4.25. Consider some polynomials

$$f(x) = a_m x^m + \cdots + a_0 \qquad g(x) = a_n x^n + \cdots + a_0 \tag{4.69}$$

Now if f, g share a factor, then we have some p, q with $\deg(p) < n$ and $\deg(q) < m$ such that $f(x)p(x) = g(x)q(x)$. In particular take

$$p \coloneqq \frac{g}{x - \alpha} \qquad q \coloneqq \frac{-f}{x - \alpha} \tag{4.70}$$

This gives us a set of linear equations for coefficients of p, q. We get a non-trivial solution when the determinant is zero. In particular our coefficients are:

$$\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_m & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_n & \cdots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & b_n & \cdots & b_2 & b_1 & b_0 \end{pmatrix} \tag{4.71}$$

[4.5] One might notice that invariants often have names ending in -ant. This is a result of James Joseph Sylvester (1814-1897) who had a habit of giving things silly names.

[4.6] This word comes from the root syn- which means together, and zygon which means yoke. Contrary to intuition, this is in fact not the longest english word without vowels. (Rhythms is.)

This matrix has $n+m$ rows. It is called the Sylvester matrix.

Definition 4.10 (Resultant)**.** The resultant is the determinant of the Sylvester matrix from above.

Example 4.26. Let f,g has a common root at ∞ if $a_m = b_m = 0$. The resultant vanishes iff f,g share a factor, possibly at infinity. Geometrically this means the projective line is complete.

Example 4.27. Consider the polynomial $f(x) = x^n - e_1 x^{n-1} + \cdots$. f has a multiple root if the resultant of f and f' vanishes. Note $\Delta = 0$ iff f has a multiple root, which means Δ should be a multiple of the resultant.

Example 4.28. We now consider the cubic curve $y^2 = x^3 + bx + c$. We might wonder when this is nonsingular. We say a curve f is *nonsingular* if $g(x,y) = 0 = f_x(x,y) = f_y(x,y)$ has no solutions, where f_x is the partial derivative with respect to x. These are the conditions that $2y = 0$, and $3x^2 + x = 0$. So $y = x^3 bx + c = 0$. Now we need to check if g, g' have a common root x. In particular, for $x^3 + bx + c$ and $3x^3 + b$ the resultant

$$\det \begin{pmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{pmatrix} \tag{4.72}$$

returns $\pm\left(4b^3 + 27c^2\right)$.[4.7]

4.6.3 Ring of invariants

Example 4.29. We might be interested in the way a finite group G acts on a complex vector space V spanned by some $\{x_1, \cdots x_n\}$. Recall that the ring of invariant polynomials is the set of polynomials $x_1, \cdots, x_n$ which is invariant under the action of G. We wonder now whether this is finitely generated over $\mathbb{C}$?

Let $G = A_n$ and $V = \mathbb{C}^n$. Then the ring is generated by $e_1, \cdots, e_n, \Delta$.

Remark 4.10. This question of generators is a computationally complicated one. When this was checked by hand, a single generator would take up many pages in a book. Hilbert luckily got around this by showing simply that the ring of invariants is always finitely generated over $\mathbb{C}$.

Definition 4.11 (Reynolds operator)**.** The *Reynolds operator*[4.8] written ρ is the average of the elements of the group:

$$\rho \coloneqq \frac{1}{|G|} \sum_{g \in G} g \tag{4.73}$$

[4.7] This sign in notoriously difficult to get right. Lang and Hilbert both made this mistake.

[4.8] Reynolds was not a mathematician at all. He studied fluid flow, and had the idea to average things over time. This turns out to be a group, and gives us this useful notion.

Remark 4.11. Polynomials in $\mathbb{C}[x_1, \cdots, x_n]$ are sent to invariants by ρ.

Example 4.30. Take $G = S_n$. Then if $f = x_1$ we have that

$$\rho(f) = \frac{x_1 + \cdots + x_n}{n} \tag{4.74}$$

Proposition 4.11. *Let ρ be the Reynolds operator. Then we have the following properties:*

1. $\rho(f+g) = \rho(f) + \rho(g)$
2. $\rho(1) = 1$
3. $\rho(fg) = \rho(f)\rho(g)$ *if* $f = \rho(g)$

Theorem 4.9 (Hilbert)**.** *Let G be a finite group. The ring of invariants of G is always finitely generated over $\mathbb{C}$.*

Proof. Look at $\mathbb{C}[x_1, \cdots, x_n]$. This is graded by degree, where $\deg(x_i) = 1$. Let I be the ring of invariants. Now define I_m to be the set of invariants homogeneous of degree m. Then we have that

$$I = \mathbb{C} \oplus I_1 \oplus I_2 \oplus \cdots \tag{4.75}$$

Look at the ideal generated by $I_1 \oplus I_2 \oplus \cdots$. By Hilbert's theorem we know this is in fact finitely generated. Take these generators to be $i_1, \cdots, i_k$. We now show that they generate the ring I.

Suppose they generate $I_1, \cdots, I_k$. We want to show that they generate I_{k+1}. Take some $f \in I_{k+1}$. Then f is an ideal J, so there are some $a_1, \cdots, a_n \in \mathbb{C}[x_1, \cdots, x_n]$ such that $f = a_1 i_1 + \cdots a_n i_n$ where $\deg(a_n) > 0$. Now we apply the Reynolds operator to get:

$$f = \rho(f) = \rho(a_1) i_1 + \rho(a_2) i_2 + \cdots + \rho(a_n) i_n \tag{4.76}$$

since f is invariant. Now we have that $\deg(a_n) < K$ since $\deg(i_n) > 0$, so by induction, $\rho(a_n)$ is a polynomial in $i_1, \cdots, i_n$. Therefore f is a polynomial in $i_1, \cdots, i_m$. □

Warning 4.2. We need to be careful showing that $i_1, \cdots i_k$ generate I.

Example 4.31. Let $R = \mathbb{C}[x, y]$ and take the subring containing the ideal generated by $x, 1$. This subring is not finitely generated as a ring.

Example 4.32. Take $G = \mathbb{Z}/n\mathbb{Z}$. Then consider the action of G on $\mathbb{C}[x, y]$. Suppose G is generated by σ such that $\sigma^n = 1$. Then we take $\xi = e^{2\pi i/n}$ and let $\sigma(x) = \xi x, \sigma(y) = \xi y$. The ring of invariants consists of the polynomials with all terms of degree $0, n, 2n, \cdots$. Then a set of $n+1$ generates is

$$\left\{x^n, x^{n-1}y, x^{n-2}y^2, \cdots\right\} \tag{4.77}$$

If we refer to these as $a_n, a_{n-1}, \cdots, a_0$ there are many relations between these a_i. For example we have that $a_n a_{n-2} = a_{n-1}^2$.

Example 4.33. We now wonder whether the collection of syzygies is finitely generated. As it turns out, it is. The ring of invariants is given by a polynomial ring in generators $a_0, \cdots, a_n$ modulo the ideal of syzygies. Then the ideal of syzygies is finitely generated by Hilbert's theorem.

4.7 Formal power series

Remark 4.12. It is important to note that these are not polynomials. We will notice throughout our analysis that many of the things we saw regarding polynomials carry over to formal power series, but we will also see places where they differ.

4.7.1 Definitions

Definition 4.12 (Formal power series ring)**.** Let R be a ring. Then we define $R[\![x]\!]$ to be the *formal power series ring* consisting of elements of the form:

$$a_0 + a_1x + a_2x^2 + \cdots \tag{4.78}$$

for $a_i \in R$.

Remark 4.13. Note polynomials are finite sums as to avoid questions of convergence, but here we ignore this, because it can be seen that you get a perfectly good ring regardless of whether a given infinite sum converges or not.

Example 4.34. Take $1 + 1!x + 2!x^2 + \cdots \in \mathbb{C}[\![x]\!]$. This only converges for $x = 0$.

Remark 4.14. In general, this doesn't give us a function from R to R.

Claim 4.1. The ring $R[\![x]\!]$ is the inverse limit of the rings $R[x]/(x^n)$ for $n \in \mathbb{Z}^+$. These are effective truncated polynomial rings. In particular $R[x]/x$ gives elements of the form a_0, $R[x]/x^2$ gives elements of the form $a_0 + a_1x$ etcetera. Then the homomorphisms of this family of rings is given by the typical map from $R[x]/x^{i+1}$ to $R[x]/x^i$ for all i.

$$R[\![x]\!] = \varprojlim R[x]/(x^n) \tag{4.79}$$

This is also called the completion of R at the ideal $I = (x)$. We can do this for a general ideal I of R, to get the object[4.9]

$$\varprojlim R/I^n \tag{4.80}$$

Warning 4.3. This example illustrates how strange completions such as this can be. In particular we find a map $R \to \varprojlim R/I^n$ which isn't injective. Take $R = \mathbb{C}\left[x^{1/n}\right]$ for all $n > 0$. then for $I = \left(x^{1/2}, x^{1/3}, \cdots\right)$ we see that $I = I^2$, so

$$R/I^n = R/I = \mathbb{C} \tag{4.81}$$

for all n, so $\varprojlim R/I^n = \mathbb{C}$.

[4.9] This if often done in number theory and algebraic geometry. See [3, 4]

Remark 4.15. Often proving a result for formal power series only involves proving it for one variable because the following relation makes it easy to generalize:

$$R\left[\!\left[x_1,\cdots,x_n\right]\!\right]=R\left[\!\left[x_1,\cdots,x_{n-1}\right]\!\right]\left[\!\left[x_n\right]\!\right] \tag{4.82}$$

Proposition 4.12. *Let k be a field and*

$$f(x)=a_0+a_1x+\cdots\in k\left[\!\left[x\right]\!\right] \tag{4.83}$$

such that $a_0\neq 0$. Then f has an inverse.

Proof. WLOG let $a_0=1$ so for some g we have $f=1+g$ and we have

$$\frac{1}{f}=\frac{1}{1+g}=1-g+g^2-g^3+\cdots \tag{4.84}$$

this makes sense since the coefficient for x^n is given by a finite sum, making it well defined for all n. □

Remark 4.16. This is our first big departure from polynomial rings.

Example 4.35. Take $f=1+x+x^2$. Then we have

$$\begin{aligned}\frac{1}{f} &= \left(1-x-x^2\right)+\left(x^2+2x^3+x^4\right)-x^3\cdots && (4.85)\\ &= 1-x+x^3-x^4 && (4.86)\end{aligned}$$

4.7.2 Ideals and condition for being Noetherian

Proposition 4.13. *Let k be a field. Then the ideals of $k\left[\!\left[x\right]\!\right]$ are $\{0\}$ and (x^n) for $n\geq 1$.*

Proof. Any element of $k\left[\!\left[x\right]\!\right]$ can be written:

$$\begin{aligned}a_nx^n+a_{n+1}x^{n+1}+\cdots &= x^n\left(a_n+a_{n+1}x+\cdots\right) && (4.87)\\ &= x^n\times\text{unit} && (4.88)\end{aligned}$$

□

Corollary 4.7. *Let k be a field. Then $k\left[\!\left[x\right]\!\right]$ is PID, UFD, and the only prime element is x.*

Proposition 4.14. *Let k be a field. Then $k\left[\!\left[x,y\right]\!\right]$ is not a PID.*

Proof. Consider the ideal (x,y). This is not principal since it is a power series without a constant term. □

Remark 4.17. Recall that $k[x,y]$ was Noetherian as a consolation for not being a PID...

Proposition 4.15. *The ring $k[x,y]$ is Noetherian.*

Theorem 4.10. *If R is Noetherian, so is $R\llbracket x\rrbracket$.*

Corollary 4.8. *If R is Noetherian, so is $R\llbracket x_1, \cdots, x_n\rrbracket$.*

Proof. We effectively turn the proof for the polynomial case upside down. Recall this proof. Let I be an ideal. Then define I_0 to be the ideal consisting of coefficients of x^0 in I, I_1 to be the coefficients of x^1 in I and so on. Then we notice that $I_0 \subseteq I_1 \subseteq \cdots$ which must stabilize since R is noetherian. Then we take polynomials of degree 0 generating I_0, polynomials of degree 1 generating I_1 and so on. until it stabilizes.

In this case we let I_0 be all elements of I, let I_1 be the smallest nonzero coefficients of x^1, so I_n is the ideal of the coefficients of x^n in series with smallest term x^n. Then $I_0 \subseteq I_1 \subseteq \cdots$ which stabilizes since R is Noetherian. Each individual ideal is finitely generated, meaning the ring is finitely generated.

Note we changed "leading" to "smallest non-zero" so in some sense we went from "down" to "up." □

4.7.3 Weierstrass preparation theorem

Theorem 4.11. *Let k be a field. Given $f \in k\llbracket x, y\rrbracket$ there exists a unit u, and g a polynomial in y with coefficients in $k\llbracket x\rrbracket$ with leading coefficient a power of x such that $f = ug$.*

Remark 4.18. An informal statement of this theorem might be as follows: Take $f \in k\llbracket x, y\rrbracket$ then we can fool x into thinking f is a polynomial. The point is we can reduce formal power series proofs to polynomial proofs.

Proof. Pick a monomial $x^m g^n$ such that $x^m y^n \neq 0$ and if $a_{b,c} = 0$ then either $a < m$ or $a = m, b < n$. If we write all the monomials in a grid, this is taking some monomial with a nonzero coefficient, and such that all the coefficients below it have zero coefficient. The idea here is kill the other coefficients of f by multiplying by units $1 + cx^i y^j$ for positive i, j and $x \in k$. So $(1 - b/a) f$ kills the coefficient of xy^3. Now we just repeat to clean the columns.

$$\begin{array}{cccc} \vdots & \vdots & \vdots & \\ 0 & a_{1,3} & a_{2,3} & \cdots \\ 0 & \boxed{a_{1,2}} & a_{2,2} & \cdots \\ 0 & 0 & a_{2,1} & \cdots \\ 0 & 0 & a_{2,0} & \cdots \end{array} \quad \rightarrow \quad \begin{array}{cccc} \vdots & \vdots & \vdots & \\ 0 & 0 & * & \cdots \\ 0 & a_{1,2} & * & \cdots \\ 0 & 0 & * & \cdots \\ 0 & 0 & * & \cdots \end{array} \tag{4.89}$$

Explicitly, multiply by $a + cx^i y^j$ so we can make the coefficients of $x^m y^k$ be zero for all $k > n$. Then we kill all the coefficients of $x^{m+1} y^k$ with $k \geq 1$. Similarly, kill off the coefficients of $x^l y^k$ with $k \geq m$. This calls off the coefficients "to the right."

So $f = xy^2 + \sum b_{ij} x^i y^j$ (up to a unit) for $i \geq m+1$ and $j \leq m$. In particular, y thinks f is a polynomial with leading term $y^2 x$. Note this unit is an infinite product which is well defined because each coefficient is only dependent on a finite calculation. So the coefficient is killing off elements in an ordering snaking from the bottom to the top of each row. It is important not to do this in another order or you might "undo" the terms you got rid of, in the sense that if you kill off $x^i y^k$ before $x^{i-k} y^{j-l}$, then when you do kill off $x^{i-k} y^{j-l}$ you might make $x^i y^j$ non-zero again. □

Corollary 4.9. *The Weierstrass preparation theorem holds for n variables. The proof is just more tedious, but holds the same form.*

Theorem 4.12. *Let k be a field. Then $k\left[\!\left[x_1, \cdots, x_n\right]\!\right]$ is a UFD.*

non-proof. We demonstrate how not to prove this theorem. A reasonable argument might be: if R is a UFD then $R\left[\!\left[x\right]\!\right]$ is a UFD. Unfortunately this is not always the case. It seems this would carry over from the polynomial case, but we need the concept of the content (which is somewhat like a gcd) and there is no such equivalent concept for a power series. For example consider $R = \mathbb{Z}$. Then we look at:

$$1 + \frac{x}{p} + \frac{x^2}{p^2} + \cdots \tag{4.90}$$

for prime p. Then the "content" of this would be $p^{-\infty} x \cdots$ which doesn't make sense. □

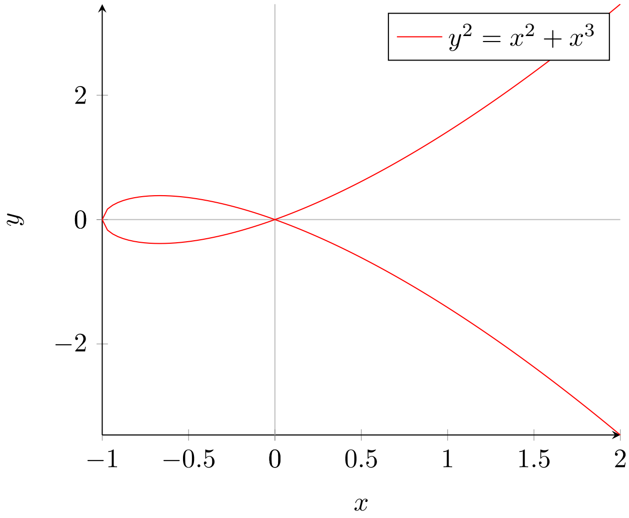
Proof. We only prove this for $k\left[\!\left[x, y\right]\!\right]$. This same method works for n variables. We first show that every element has a factorization into irreducibles. The proof for $R\left[x\right]$ works for any Noetherian ring, and $R\left[\!\left[x\right]\!\right]$ is Noetherian.

We now show uniqueness. The key step is that irreducible implies prime here. Suppose $f | gh$. Then by Weierstrass we can assume $f, g, h \in k\left[\!\left[x\right]\!\right]\left[y\right]$ since multiplying by a unit doesn't change divisibility. Now notice $k\left[\!\left[x\right]\!\right]\left[y\right]$ is a UFD. This is because $k\left[\!\left[x\right]\!\right]$ is a UFD itself (this is done by induction in the case of n variables). So $f | g$ or $f | h$ in $k\left[\!\left[x\right]\!\right]\left[y\right]$ and therefore in $k\left[\!\left[x\right]\!\right]\left[\!\left[y\right]\!\right]$. □

Example 4.36. Let k be a ring of characteristic 0. Consider the ring $k\left[x, y\right]$ and $f\left(x\right) = y^2 - x^2 - x^3$ which is irreducible. To see this, note that $x^2 - x^3$ is not a square of anything. But now consider f in $k\left[\!\left[x, y\right]\!\right]$. It is reducible in this ring, because we can write:

$$y^2 - x^2 - x^3 = \left(y + x\sqrt{1+x}\right)\left(y - x\sqrt{1+x}\right) \tag{4.91}$$

which is a formal power series since we can expand $\sqrt{1+x} = 1 + \frac{1}{2}x + \cdots$ We can understand this using some geometric intuition. We can plot this curve as:



(4.92)

Then if we imagine only considering this curve as it is seen in a small neighborhood of the origin, we see this curve divided into two lines gives by our factorization above.

4.7.4 Hensel's Lemma

Lemma 4.5 (Hensel's)**.** *Suppose $f(x,y) \in k[\![x,y]\!]$, and that the smallest nonzero coefficients are of degree d and for a polynomial $f_d(x,y)$. Suppose $f_d = gh$ where g,h are coprime. Then $f = GH$ where g,h are the smallest d degree terms of G,H.*[4.10]

Remark 4.19. This is lifting a rough factorization to the whole thing.

Example 4.37. Consider $f(x,y) = y^2 - x^2 + x^3$, $d = 2$, and $f_d(x,y) = y^2 - x^2 = (y-x)(y+x)$. This lifts to:

$$y^2 = x^2 - x^3 = (y - x + \cdots)(y + x + \cdots) \tag{4.93}$$

then the first term here corresponds to $y - x\sqrt{1+x}$ and the second to $y + x\sqrt{1+x}$.

Example 4.38. We now consider a situation where a factorization doesn't lift. Consider $y^2 - x^3$ and $d = 2$. Then $f_d(x,y) = y^2 = y \times y$ but $y^2 - x^3$ does not factorize. This plot is just a cusp rather than the loop.

Remark 4.20. The power series rings are analogous to the p-adic rings since as we recall,

$$\mathbb{Z}_p := \varprojlim (\mathbb{Z}/p^n) \tag{4.94}$$

[4.10] There are many different versions of this lemma. One of which applied to p-adic integers which we will see shortly.

Lemma 4.6 (Hensel's lemma for p-adic integer)**.** *Let $f \in \mathbb{Z}[x]$. Suppose $f(x) = 0$ has a root modulo p. If $f'(x) \neq 0 \pmod{p}$ then $f(x) = 0$ has root in $\mathbb{Z}_p$. This means $f(x) = (x-a)\, g(x)$. Also $f(x) \equiv 0 \pmod{p^n}$ has root for all $n \geq 1$. This means $(x-a)$ and g are coprime.*

Example 4.39. This example is comparable to the case of $y^2 - x^2 - x^3$ factoring. Consider $f(x) = x^2 - 7$ and $p = 3$. Then $f(1) = 1^2 - 7 \equiv 0 \pmod{3}$ and $f'(1) = 2 \not\equiv 0 \pmod{3}$ so $x^2 - 7 \equiv 0 \pmod{p^n}$ has a root for all $n \geq 1$.

Example 4.40. This example is analogous to the case of $x^2 - x^3$ not factoring. Take $f(x) = x^2 - 7$ and $p = 2$. Then $f(1) \equiv 0 \pmod{2}$ but $x^2 - 7$ has no roots modulo $2^3 = 8$ since $f'(1) \equiv 0 \pmod{2}$.

Chapter 5

Algebraic extensions

5.1 Field extensions

Definition 5.1 (Field extension)**.** Let K be a field. A field L is a *field extension* of K iff K is a subfield of L, written:

$$K \subseteq L \qquad \text{or} \qquad L/K \tag{5.1}$$

Definition 5.2 (Degree)**.** Let L be an extension of K. Then the degree $[L : K]$ of L/K is $\dim L$ as a vector space over K.

Example 5.1. The complex numbers $\mathbb{C}$ are a field extension of $\mathbb{R}$, where $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 5.3 (Algebraic)**.** An element $\alpha \in L$ is algebraic over K iff it is the root of a polynomial in $K[x]$.

Example 5.2. The number $\sqrt[5]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ as a root of $x^5 - 2$.

Example 5.3. The real numbers π, e are both not algebraic over $\mathbb{Q}$. This is called *transcendental*. This is hard to prove. See the appendix to Lang [5].

Remark 5.1. It is typically hard to prove something is not algebraic. For example, we don't know whether $\pi + e, \pi e$ are algebraic.

Example 5.4. Let $L = \mathbb{Q}(x)$ denote the rational functions in x. Then we have that $[L : \mathbb{Q}] = \infty$ and x is not algebraic.

Proposition 5.1. *Let p be an irreducible polynomial. Then $K[x]/p(x)$ is a field.*

Proof. Consider the ideal generated by p. Since p is irreducible, this ideal is maximal among the principal ideals of $K[x]$. Since $K[x]$ is a PID, this means (p) is maximal in general, and therefore $K[x]/(p)$ is a field. □

Remark 5.2. This is not true for a polynomial in more than one variable because we do not have that $K\left[x_1, \cdots, x_n\right]$ is a PID.

Theorem 5.1. *α is algebraic over K iff it is contained in some finite extension K_1 of K, so we can write $\left[K_1 : K\right] < \infty$.*

Proof. Let $\alpha \in K_1$ such that $\left[K_1 : K\right] = n < \infty$. Then we look at the powers $1, \alpha, \alpha^2, \cdots, \alpha^n$. This is a collection of $n+1$ elements from an n-dimensional vector space over K, meaning we can write

$$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_n\alpha^n = 0 \tag{5.2}$$

for some $\{a_j\} \subseteq K_i$ not all zero meaning α is algebraic.

Now suppose $\alpha \in L$ is algebraic over K. Then we have some $p \in K\left[x\right]$ such that $p\left(\alpha\right) = 0$. WLOG take p to be irreducible, meaning $K_1 \coloneqq K\left[x\right] / \left(p\right)$ is a field by the preceding lemma. Then we have $\left[K_1 : K\right] = \deg\left(p\right)$ with basis $\left\{1, x, \cdots, x^{\deg(p)-1}\right\}$. This gives us a map $\varphi : K\left[x\right] / \left(p\right) \to L$ where $x \mapsto \alpha$.

$$\begin{tikzcd}
K_1 \arrow[r, "\varphi"] & L \\
K \arrow[u] \arrow[ur] &
\end{tikzcd} \tag{5.3}$$

Note that φ is injective and K_1 is a field, so $\operatorname{im}\left(\varphi\right)$ is a field of finite degree containing α. □

Lemma 5.1. *Let $K \subseteq K_1 \subseteq K_2$. Then we have*

$$\left[K_2 : K\right] = \left[K_2 : K_1\right]\left[K_1 : K\right] \tag{5.4}$$

Proof. Take $\{x_1, \cdots, x_m\}$ to be a basis of K_1 over K. Take $\{y_1, \cdots, y_n\}$ to be a basis of K_2 over K_1. Then we have that $x_i y_j$ forms a basis of K_2 over K, so $\left[K_2 : K\right] = mn$ as desired. □

Proposition 5.2. *Let $\alpha, \beta \in L$ be algebraic over K. Then $\alpha + \beta$ and $\alpha\beta$ are also algebraic over K.*

Proof. Take $\alpha \in K_1$ and $\left[K_1 : K\right] < \infty$. We know that β is the root of some irreducible polynomials of finite degree n over K_1, so β is algebraic over K. In particular, let $\beta \in K_2$ where $\left[K_2, K_1\right] < \infty$. Then from lemma lemma 5.1 we have that

$$\left[K_2 : K\right] = \left[K_2 : K_1\right]\left[K_1 : K\right] \tag{5.5}$$

so $\left[K_2, K\right] < \infty$ as well, so since $\alpha\beta, \alpha + \beta \in K_2$ we have the desired result. □

Example 5.5. The number $\sqrt{2} + \sqrt[3]{2} + \sqrt[5]{2}$ is algebraic over $\mathbb{Q}$ since the individual terms are. This is easy to see this way, but if were to attempt to do this directly, we would need to find the polynomial which had this number as a root. Such a polynomial has at least a degree of 30.

Example 5.6. The algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$ form a field. This is called the field of algebraic numbers, particularly in the field of algebraic number theory.

Remark 5.3. We have been considering $K[x]/(p)$ for irreducible p frequently here. If p is not irreducible, we have $p = fg$ and if f, g are coprime, we have that

$$K[x]/(p) = K[x]/(g) \times K[x]/(h) \tag{5.6}$$

by the Chinese remainder theorem. This means, as long as p does not have repeated factors, $K[x]/(p)$ is a product of fields. If it does have repeated factors, we can be dealing with something very strange.

Example 5.7. Let $p = x^n$. Then $K[x]/(p)$ is the field of truncated polynomials up to and not including degree n. In particular have $x^n = 0$. We have nilpotent elements in this, so it cannot be a product of fields.

Proposition 5.3. *Let $p \in K[x]$ be irreducible. We can find an extension field $L \supseteq K$ such that p has a root in L.*

Proof. Take $L = K[x]/(p)$. □

Example 5.8. We provide an example of a polynomial p such that p has a root in $K[x]/(p)$ but does not factorize into linear factors. Consider: $\mathbb{Q}[x] \ni p(x) = x^3 - 2$ which is irreducible by Eisenstein's criterion. Then we have

$$L = \mathbb{Q}[x]/(p) \cong \mathbb{Q}\left[\sqrt[3]{2}\right] \tag{5.7}$$

All the elements of L are of the form $a_0 + a_1\sqrt[3]{2} + a_2\left(\sqrt[3]{2}\right)^2$ for $a_i \in \mathbb{Q}$. However p still does not factorize linearly in L. In particular, $L \subseteq \mathbb{R}$, and p only has one real root. The other two roots are:

$$\sqrt[3]{2}e^{4\pi i/3} \qquad \sqrt[3]{2}e^{2\pi i/3} \tag{5.8}$$

Example 5.9. Consider $p(x) = x^4 + 1$. To see this is irreducible, consider that $p(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ which allows us to apply Eisenstein's criterion. Now we have the complex roots:

$$e^{\pi i/4} \qquad e^{3\pi i/4} \qquad e^{5\pi i/4} \qquad e^{7\pi i/4} \tag{5.9}$$

Then we have that

$$L = \mathbb{Q}[x]/\left(x^4+1\right) \cong \mathbb{Q}[\zeta] = \left\{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^4 : a_i \in \mathbb{Q}\right\} \tag{5.10}$$

so p factors as:

$$p(x) = (x-\zeta)\left(x-\zeta^3\right)\left(x-\zeta^5\right)\left(x-\zeta^7\right) \tag{5.11}$$

5.2 Splitting fields

Definition 5.4. Let $p \in K[x]$ with $K \subseteq L$. Then L is a splitting field of p iff

1. p factors linearly in L
2. L is generated by roots of p

Example 5.10. If ζ is such that $\zeta^4 = -1$ then $\mathbb{Q}[\zeta]$ is a splitting field of $p = x^4 + 1$.

Example 5.11. $\mathbb{Q}\left[\sqrt[3]{2}\right]$ is not a splitting field of $p = x^3 - 2$. We seek to construct a splitting field given a polynomial $p = x^3 - 2$. First we find

$$K_1 = \mathbb{Q}\left[2^{1/3}\right] = \mathbb{Q}[x] / (p) \tag{5.12}$$

then as considered in K_1, $p = \left(x - 2^{1/3}\right)\left(x^2 + 2^{1/3}x + 2^{2/3}\right)$ now we add the roots of this to K_1 to get

$$K_2 = \mathbb{Q}[x] / \left(x^2 + 2^{1/3}x + 2^{2/3}\right) \tag{5.13}$$

We continue like this. We give the general procedure in the next example.

Example 5.12. Given a polynomial $p \in K[x]$, we can form its splitting field as follows: Factor p. If all the factors are linear, we are done. If not, we take a non-linear irreducible factor q and form $K_1 = K[x] / (q)$. Repeat this with p/q to get

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \tag{5.14}$$

where at a certain degree k, we add the root α_k of the polynomial

$$p / \left[(x - \alpha_1) \cdots (x - \alpha_{k-1})\right] \tag{5.15}$$

This gives that

$$[K_n : K] \leq n! \tag{5.16}$$

making use of lemma 5.1. This gives us that the splitting field is effectively unique.

Proposition 5.4. *Let L_1, L_2 be two splitting fields of a field K. Then we can find an isomorphism from L_1 to L_2 fixing all elements of K.*

$$\begin{tikzcd} L_1 \arrow[r] & L_2 \\ K \arrow[u] \arrow[ur] & \end{tikzcd} \tag{5.17}$$

This isomorphism is not necessarily unique.

Proof. As before, we construct a sequence of splitting fields

$$K \subseteq K_1 \subseteq K_2 \cdots \subseteq K_n \tag{5.18}$$

Let L be a splitting field of K. Then we get a map $\varphi_1 : K_1 \to L$ since $K_1 = K[x]/(q_1)$ and L is a splitting field of p. Then we can form such maps for each K_i to get

$$\begin{tikzcd}
K \arrow[d] & K_1 \arrow[dl, "\varphi_1"] & \cdots & K_n \arrow[dlll, "\varphi_n"] \\
L & & &
\end{tikzcd} \tag{5.19}$$

Now we know the $\operatorname{im}(\varphi_n) = L$ since L is generated by the roots of p by definition. As such, $K_n \cong L$. □

Example 5.13. To see that this isomorphism is not necessarily unique, consider the splitting field of $x^2 + 1$ over $\mathbb{R}$. This happens to be $\mathbb{C}$. But what is $\sqrt{-1}$? Depending on the particular isomorphism, it could be either $\pm i$.

5.2.1 Finite fields

Proposition 5.5. *For any prime power p^n there is a unique field F_{p^n} with p^n elements.*

Proof. The main idea here is that F_{p^n} is the splitting field of the polynomial $x^{p^n} - x$. We first show that such a splitting field does in fact have p^n elements. We know $x^{p^n} - x$ has p^n distinct roots because the derivative of this polynomial is $px^{p^n-1} - 1$ which is coprime to $x^{p^n} - x$. The main point here is that the roots form a field, since they are closed under addition and multiplication. To see this, note that $(x+y)^p = x^p + y^p$ and that the roots are either 0 or roots of $x^{p^n-1} = 1$. So the roots form a field of order p^n.

We now show uniqueness. To do this we show that any field of order p^n is a splitting field of $x^{p^n} - x$. The key point here is that all elements of such a field must be roots of this polynomial. In particular, if $x = 0$, it is a root, and if not, $x \in L^\times$. But $L^\times$ is a group of order $p^n - 1$, so $x^{p^n-1} = 1$ by Lagrange's theorem. □

Example 5.14. What is the field of order 2^4? We can use the previous proposition. The proof shows it exists, but is useless for the actual construction. To do this, first find some irreducible factor p of the polynomial $x^{2^4} - x$ of degree 4, and take $F_2[x]/(p)$. This is clearly a field of order 16. Furthermore, any field of order 16 is such a splitting field. We also know that any irreducible polynomial of degree 4 divides $x^{16} - x$, so we write:

$$\begin{aligned}
x^{16} - x &= \left(x^4 + x^3 + x^2 + 1\right)\left(x^4 + x^3 + 1\right)\left(x^4 + x + 1\right) && (5.20)\\
&\quad \left(x^2 + x + 1\right)(x+1)\,x && (5.21)
\end{aligned}$$

These irreducible polynomials were derived in a previous example. This is divisible by $x^{2^2} - 1$ and $x^{2^1} - 1$. To get an explicit construction of this, consider

$F_2[x]/\left(x^4+x+1\right)$. In general we can take any fourth degree irreducible polynomial, and there is no a priori preference.

Example 5.15. We seek to find all the irreducible polynomials of degree 6 in $F_2[x]$. To see this, we know we can write:

$$\begin{aligned} x^{2^6} &= (\text{irred. polys of deg 6})\,(\text{irred. polys of deg 3}) \qquad (5.22)\\ &\quad (\text{irred. polys of deg 2})\,(x+1)\,x \qquad (5.23)\end{aligned}$$

using an inclusion-exclusion argument we have that the degree of the product of the polynomials of degree 6 is $2^6-2^3-2^2+2^1$. Then dividing through by degree 6, we get the number of polynomials as $\left(2^6-2^3-2^2+2^1\right)/6=8$.

5.3 Algebraic closure

Definition 5.5. $L\supseteq K$ is called the algebraic closure of K iff

1. Every element of L is algebraic over K.
2. Every polynomial in $L[x]$ has a root.

Example 5.16. The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Proposition 5.6. *Let K be a field. Then K has an algebraic closure L unique up to isomorphism. Furthermore, given any set of polynomials in $K[x]$ we can find a splitting field such that*

1. *All such polynomials factorize linearly.*
2. *L is generated by the roots of the polynomials.*

Proof. Let there be some countable family of polynomials $\{p_i\}_{i\in\mathbb{N}}$. Then we can form

$$K\subseteq K_1\subseteq K_2\subseteq\cdots \qquad (5.24)$$

where K_i is a splitting field of p_i over K_{i-1}. Then notice that the union of the K_i is also a splitting field. On the other hand, if we have an uncountable number of polynomials p_i, we use the magic words: Zorn's lemma. So we have found $L\supseteq K$ such that any polynomial in $K[x]$ has a root in L. But we still need to show that all polynomials in $L[x]$ have a root in L.

Suppose that p is irreducible in $L[x]$. Now consider $M:=L[x]/(p)$. So the coefficients of p are all in K, and therefore are in some finite extension of K. This means α is in some finite extension of K, and is therefore algebraic over K. Therefore $\alpha\in L$, since any polynomials in $K[x]$ factorizes linearly in L.

Uniqueness is similar to the case of splitting fields. We leave this as an exercise. □

Remark 5.4. It is hard to find simple examples of algebraic closure.

Example 5.17. Let K be the field of formal Laurent series over $\mathbb{C}$. This has elements:

$$\cdots + a_{-n}x^{-n} + \cdots + a_{-1}x^{-1} + a_0 + a_1x^1 + \cdots a_nx^n \cdots \tag{5.25}$$

for $a_i \in \mathbb{C}$. Then the algebraic closure L of K is

$$L = \bigcup_{k\geq 1} \text{Laurent series in } x^{1/k} \tag{5.26}$$

These are called Puiseux series.[5.1]

5.4 Normal extensions

Proposition 5.7. *A field L is a splitting field for some family of polynomials iff an irreducible polynomial having one root in L implies it has all roots in L.*

Proof. Let $p \in K[x]$ be an irreducible polynomial with a root $\alpha \in L$. Let M be the algebraic closure of L. Any homomorphism $\varphi : K[\alpha] \to M$ extends to a homomorphism $\psi : L \to M$ since M is algebraically closed. Furthermore, $\operatorname{im}(\psi) = L$ since L is the splitting field of some family of polynomials in $K[x]$. In particular, the splitting field is a uniquely determined subfield of M, since it is generated by a family of polynomials. Therefore α is already in L. □

Example 5.18. The result we saw in proposition 5.7 holds for irreducible polynomials. This is however not true for any polynomial. For example, consider $K = \mathbb{Q}$ and $L = \mathbb{Q}\left(\sqrt[3]{2}\right)$. Then $x^3 - 2$ has a root in L, but does not split into linear factors.

Definition 5.6. A finite field extension L/K is *normal* iff the existence of 1 root of an irreducible polynomial p implies the existence of all the roots of p in L.

Proposition 5.8. *An extension L/K is normal iff it is the splitting field of some family of polynomials.*

Proof. This follows directly from definition 5.6 and proposition 5.7. □

Proposition 5.9. *A finite field extension L/K is normal iff it is the splitting field of some family of polynomials.*

Proposition 5.10. *Let L/K be a field extension. If $[L : K] = 2$ then L is normal.*

Proof. Let α be a root of a polynomial $a^2 + ax + b = (a - \alpha)(a - \beta)$. Then we have $\alpha + \beta = -a$ meaning $\beta = -a - \alpha$ so $\beta \in K[\alpha]$ as desired. □

[5.1] These date back to Newton, but no one knew what Algebraic closure was back then.

Example 5.19. The extension $\mathbb{Q}\left[\sqrt[3]{2}\right]/\mathbb{Q}$ is not normal. To see this, consider: $x^2 - 2 = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \left(\sqrt[3]{2}\right)^2\right)$.

Warning 5.1. Normal extensions of normal extensions are not always normal over the original base field.

Example 5.20. As an example of a normal extension of a normal extension which is not normal with respect to the base field consider $\mathbb{Q}\left[\sqrt[4]{3}\right]/\mathbb{Q}$ which is not normal over $\mathbb{Q}\left[\sqrt{2}\right]/\mathbb{Q}$ but it is over $\mathbb{Q}\left[\sqrt[4]{2}\right]/\mathbb{Q}\left[\sqrt{2}\right]$ which is normal over $\mathbb{Q}\left[\sqrt{2}\right]/\mathbb{Q}$.

5.5 Separable extensions

Definition 5.7. A polynomial p is called *separable* iff it has no repeated roots.

Proposition 5.11. *Let p be a polynomial. Then p is separable iff p, p' are coprime.*

Definition 5.8. Let L/K be a field extension. $\alpha \in L$ is *separable* iff its irreducible polynomial is separable.

Definition 5.9. A field extension L/K is *separable* iff all of the elements are separable.

Theorem 5.2. *Let L/K be a field extension. If K has characteristic 0, then L/K is separable.*

Proof. Let α be a root of some irreducible polynomial p. Then $\deg(p) > \deg(p')$ so p, p' have no common factors since p is irreducible. Therefore p, p' are coprime as desired. □

Remark 5.5. It is not immediately clear why we might need the field to have characteristic 0 in the preceding proof. The point is, if $p' = 0$, unless the field does indeed have characteristic 0, this does not necessarily imply that p is constant.[5.2]

Corollary 5.1. *Any extension F_q/F_p of finite fields is separable.*

Proof. Any element is a root of the polynomial $p(x) = x^q - x$ which just has derivative $p'(x) = -1$ so $(p, p') = 1$. □

Example 5.21. We offer an example of an extension which is not separable. Consider $F_p(t)$ the rational functions in t. We have that $F_p(t^p) \subseteq F_p(t)$ so if $p(x) = x^p - t^p$ then $p(t) = 0$. We have $(a+b)^p = a^p + b^p$ in this field so p factors as $(x-t)^p$ so all p roots are identical. As such, t cannot be the root of separable polynomial in $F_p(t)[x]$.

[5.2] Maybe it does in analysis...

5.6 Galois extensions

Definition 5.10. A field extension is Galois[5.3] iff it is separable and normal.

Definition 5.11. Let L/K be a Galois extension. The *Galois group* of L/K written $\operatorname{Gal}(L, K)$ is the group of automorphisms of L fixing K.

Remark 5.6. In some sense, G controls the extension L/K. This means that some questions and theorems about fields can be transformed into questions and theorems about groups.

Lemma 5.2. *Let L/K be a finite extension of degree n. Then there are at most n ways to get a map f such that*

$$\begin{tikzcd} L \arrow[r, "f"] & M \\ K \arrow[u] \arrow[ur] & \end{tikzcd} \tag{5.27}$$

Proof. Suppose L is generated by α so $L = K[\alpha]$. Then α is a root of some polynomial p of degree $\leq n$. $f(\alpha)$ is also such a root in M but p has at most n roots. □

Theorem 5.3. *Let L/K be a finite extension. Then TFAE:*

1. *L is a splitting field of a separable polynomial*
2. *L is Galois*
3. *$[L : K] = |G|$ where G is the group of automorphisms of L fixing the elements of K. This is called the Galois group.*
4. *$K = L^G$ is the elements of L fixed by G.*

Proof. (1) $\implies$ (2): All splitting fields are normal.

(2) $\implies$ (3): Take $K \subseteq L \subseteq M$ where M is the algebraic closure of K. Look at the maps taking $L \to M$ which extend the identity map on K. We know L/K is separable, so there are $[L : K] = n$ such extensions. This is because L is generated by α of degree n. We can map α to any root of p in M, and P has n roots as it is separable. We leave the case where L is not generated by 1 element as an exercise. L/K is normal, so the image of any map from L to M lies in L. So there are $\geq n$ maps from $L \to L$ which fix K. From lemma 5.2 we have that there are always $\leq [L : K]$ maps from $L \to L$ so $|G| = [L : K]$.

(3) $\implies$ (4): Consider $K \subseteq L^G \subseteq L$. There are $\geq n$ automorphisms of L extending L^G. Therefore $\left[L : L^G\right] \geq n$, but we also know $[L : K] = n$ so $K = L^G$.

[5.3] Tom Lehrer once said "It is sobering to consider that when Mozart was my age he had already been dead for two years." The same might be said by a 22 year old Mathematician about Galois.

(4) $\implies$ (1): Let $\alpha \in L$ and consider the conjugates of α under $G = \mathrm{Gal}\left(L/K\right)$. Look at $\left(x-\alpha\right)\left(x-\beta\right)\left(x-\gamma\right)\cdots$. This is in $K\left[x\right]$ as all coefficients are invariant under G, since $K = L^G$. So α is a root of a separable polynomial, since $\alpha, \beta, \gamma, \cdots$ are distinct. The polynomial splits into linear factors, which gives us that the extension is normal as desired. □

Remark 5.7. By lemma 5.2, the third statement can be interpreted as meaning L is "as symmetric" as it can be.

Example 5.22. Take $p\left(x\right) = x^3 - 2$ to be a rational polynomial. p has three roots: $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ where $\omega^3 = 1$.

Now take L to be the splitting field of p. Then we have that $[L : \mathbb{Q}] = 6$ since

$$\left[L : \mathbb{Q}\left[\sqrt[3]{2}\right]\right] = 2 \qquad\qquad \left[\mathbb{Q}\left[\sqrt[3]{2}\right] : \mathbb{Q}\right] = 3 \tag{5.28}$$

which means $G = \mathrm{Gal}\left(L, \mathbb{Q}\right)$ has order $[L : \mathbb{Q}] = 6$. In particular G acts as the permutations of the three roots, so $G = S_3$.

Example 5.23. Consider the ring $\mathbb{C}/\mathbb{R}$. Then $\mathrm{Gal}\left(\mathbb{C}/\mathbb{R}\right)$ has order 2 and is generated by complex conjugation. It permutes roots of $z^2 + 1 = 0$.

Remark 5.8. Finding the Galois group of a ring is somewhat like generalized complex conjugation.

Example 5.24. The ring F_{16}/F_2 is the splitting field of $x^{16} - x$ so $\mathrm{Gal}\left(F_{16}/F_2\right)$ should have order $4 = [F_{16} : F_2]$. But what does it look like? Well we know one element: the Frobenius element. We call this element φ. We have that $\varphi\left(a\right) = a^2$ so $\varphi\left(ab\right) = \varphi\left(a\right)\varphi\left(b\right)$ and $\varphi\left(a+b\right) = \varphi\left(a\right) + \varphi\left(b\right)$. If $\varphi\left(a\right) = a^2 = a$ then $a = 1$ or $a = 0$. Therefore $a \in F_3$, so φ generated the Galois group, and $\varphi^4\left(a\right) = a^{16} = a$ is the identity. Therefore $\mathrm{Gal}\left(F_{16}, F_2\right) = \mathbb{Z}/4\mathbb{Z}$.

5.7 Main theorem of Galois theory

Theorem 5.4. *Let M/K be a Galois extension and G denote the Galois group $\mathrm{Gal}\left(M, K\right)$. We have a correspondence between sub-extensions L where $K \subseteq L \subseteq M$ and subgroups $H \subseteq G$. Explicitly we send*

$$L \mapsto \mathrm{Gal}\left(M/L\right) \qquad\qquad M^H \mapsfrom H \tag{5.29}$$

where M^H is the set of elements of M fixed by H.

Proof. We have the following diagrams:

$$\begin{tikzcd}
L \arrow[dr] \arrow[dd, hook] & & & H \arrow[dl] \arrow[dd, hook] \\
& \mathrm{Gal}\left(M/L\right) \arrow[dl] & M \arrow[dr] & \\
M^{\mathrm{Gal}\left(M/L\right)} & & & \mathrm{Gal}\left(M/M^H\right)
\end{tikzcd} \tag{5.30}$$

Now we want to show these embeddings are actually equalities. It is enough to show they have the same "size." In the first case we interpret this to mean they have the same index in M and in the second case we interpret this to mean they have the same order as groups.

Warning 5.2. It might be tempting to measure the size of the fields by the index of K inside them instead, but this will not be sufficient.

In summary, the main theorem follows if we show:

1. $|\mathrm{Gal}\,(M/L)| = [M : L]$
2. $\left[M : M^H\right] = |H|$

(1): Recall that if $K \subseteq L \subseteq M$, there are $\leq [L : K]$ maps from $L \to M$ extending the inclusion map of K. As a result, $|\mathrm{Gal}\,(M/L)| \leq [M : L]$. To see that this is in fact an equality, we assume the inequality is strict. Look at $K \subseteq L \subseteq M$. There are $\leq [L : K]$ extension maps from L to M and $\leq [M : L]$ extension maps from M to M, so in total there are less than $[L : K]\,[M : L] = [M : K]$ maps from M to M. But since M/K is a Galois extension there are $[M : K]$ maps from M to M so $|\mathrm{Gal}\,(M/L)| \leq [M : L]$ as desired. The other item is left as an exercise. □

Remark 5.9. This proof is strange because it's unusually abstract, and doesn't really use anything about groups or fields in the actual proof.

Warning 5.3. The above bijection reverses inclusions. Bigger subfields correspond to smaller subgroups. Note that L is mapped to $\mathrm{Gal}\,(M/L)$ and not $\mathrm{Gal}\,(L/K)$. After all, $\mathrm{Gal}\,(L/K)$ is not even a subgroup of $\mathrm{Gal}\,(M/K)$ in general.

Example 5.25. Here is another confusing example of Galois correspondence. Let $K \subseteq L \subseteq M$ where L, M are both Galois extensions of K. Then $\mathrm{Gal}\,(M/K)$ is bigger than $\mathrm{Gal}\,(L/K)$. Here bigger implied bigger...

5.8 Intermediate field extensions

Example 5.26. Find all intermediate fields between $\mathbb{Q}$ and the splitting field of $x^3 - 2$. This should be of degree 6, and generated by

$$\sqrt[3]{2},\ \sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2, \tag{5.31}$$

where $\omega^3 = 1$. Look at the Galois group S_3. Then we have that the correspondence explicitly gives:

$$\begin{tikzcd}
& S_3 \arrow[dl, dash, "3"'] \arrow[d, dash, "3"] \arrow[dr, dash, "3"] \arrow[drr, dash, "2"] & & \\
(12) \arrow[dr, dash, "2"'] & (23) \arrow[d, dash, "2"] & (31) \arrow[dl, dash, "2"] & (123), (132) \arrow[dll, dash, "3"] \\
& \{e\} & &
\end{tikzcd} \tag{5.32}$$

$$\begin{tikzcd}
& \mathbb{Q} \arrow[dl, dash, "3"'] \arrow[d, dash, "3"] \arrow[dr, dash, "3"] \arrow[drr, dash, "2"] & & \\
\mathbb{Q}\left(\sqrt[3]{2}\omega^2\right) \arrow[dr, dash, "2"'] & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[d, dash, "2"] & \mathbb{Q}\left(\sqrt[3]{2}\omega\right) \arrow[dl, dash, "2"] & \mathbb{Q}(\omega) \arrow[dll, dash, "3"] \\
& \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega\right) & &
\end{tikzcd} \tag{5.33}$$

the indices of the subgroups correspond to the degrees of the subextensions.

Example 5.27. Let ζ be a 7th root of unity in $\mathbb{C}$. Then $\zeta^7 = 1$ and

$$\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0 \tag{5.34}$$

is irreducible. What is the corresponding splitting field? Well we can take the polynomial

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x - \zeta)\left(x - \zeta^2\right) \cdots \left(x - \zeta^6\right) \tag{5.35}$$

so $\mathbb{Q}[\zeta]$ is normal of degree 6. But what are all the subfields? First notice: $G = \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^\times$ which is cyclic of degree 6. The elements of this group are:

3^0	3^1	3^2	3^3	3^4	3^4
1	3	2	6	4	5

then the correspondence between subgroups of G and subfields of our extension gives us the following:

$$\begin{tikzcd}
& \{1\} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & & & \mathbb{Q}[\zeta] \arrow[dl, dash] \arrow[dr, dash] & \\
\{1,2,4\} \arrow[dr, dash, "2"'] & & \{1,6\} \arrow[dl, dash, "3"] & L_2 \arrow[dr, dash] & & L_3 \arrow[dl, dash] \\
& G & & & \mathbb{Q} &
\end{tikzcd} \tag{5.36}$$

where we know L_2 to be a field of degree 2, and L_3 of degree 3. We now desire to find these fields explicitly. First call $H = \{1, 2, 4\}$. To find a fixed element of this group, simply take

$$a = \zeta^1 + \zeta^2 + \zeta^4 = \sum_{\sigma \in H} \sigma(\zeta) \tag{5.37}$$

so $L_2 = \mathbb{Q}[a] = \mathbb{Q}\left[\zeta + \zeta^2 + \zeta^4\right]$. But what actually is a? We want a more explicit form for this field. Well we can write:

$$\begin{aligned} a^2 &= \zeta^2\zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 && (5.38) \\ &= \zeta + \zeta^2 + 2\zeta^3 + \zeta^4 + 2\zeta^5 + 2\zeta^6 && (5.39) \\ &= 2\left(\zeta + \zeta^2 + \cdots + \zeta^6\right) && (5.40) \\ &= -2 && (5.41) \end{aligned}$$

so for $p(x) = x^2 + x + 2$ we have $p(a) = 0$. Therefore $a = \left(-1 + \sqrt{-7}\right)/2$ and $L_2 = \mathbb{Q}\left[\sqrt{-7}\right]$.

We now desire to do the same for L_3. As before, take $J = \{1, 6\}$ and find a fixed element

$$b = \sum_{\sigma \in J} \sigma(x) \tag{5.42}$$

for any x. In particular we can take $x = \zeta$ to get $b = \zeta + \zeta^6 = \zeta + \zeta^{-1}$ in our field. Then by inspection $\zeta = \exp(2\pi i/7) = \cos(2\pi/7) + i\sin(2\pi/7)$ which means $b = 2\cos(2\pi/7)$ and $L_3 = \mathbb{Q}[2\cos(2\pi/7)]$. This lets us write

$$\begin{aligned} b^3 &= \left(\zeta + \zeta^{-1}\right)^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} && (5.43) \\ b^2 &= \left(\zeta + \zeta^{-1}\right)^2 = \zeta + 2 + \zeta^{-1} && (5.44) \end{aligned}$$

so since $\zeta^3 + \zeta^2 + \zeta + \cdots + \zeta^{-3} = 0$, if $p(x) = x^3 + x^2 - 2x - 1$ then $p(b) = 0$ and $L_3 = \mathbb{Q}[x] / \left(x^3 + x^2 - 2x - 1\right)$. Note $2\cos(2\pi/7), 2\cos(4\pi/7), 2\cos(8\pi/7)$ are the three roots of p.

Example 5.28. We can apply the main theorem of Galois theory to see how to construct a 17 sided regular polygon with ruler and compass.[5.4] We want ζ such that $\zeta^{17} = 1$. This gives us the vertices of such a polygon on the unit disk. In particular take $\zeta = \exp(2\pi i/17)$. Recall that

$$p(x) = \frac{\zeta^{17} - 1}{\zeta - 1} \tag{5.45}$$

is irreducible of degree 16 such that $p(\zeta) = 0$. So the idea is to construct fields:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\zeta) \tag{5.46}$$

all extensions of degree 2. As it turns out, you can always find extensions of degree 2 with ruler and compass. This isn't too hard to do, since as we

[5.4] This construction made Gauss famous as a teenager.

have seen these subextensions correspond to subgroups of our Galois group $G = (\mathbb{Z}/17\mathbb{Z})^\times = \mathbb{Z}/16\mathbb{Z}$. The subgroups of G are:

$$0 \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/8\mathbb{Z} \subseteq \mathbb{Z}/16\mathbb{Z} \tag{5.47}$$

so some fixed fields give a tower of extensions. But what are they? Look at $\mathbb{Z}/16\mathbb{Z}$. The powers of 3 modulo 17 are:

0	1	2	3	4	5	6	7	8
$\boxed{1}$	③	9	10	$\boxed{13}$	⑤	15	11	$\boxed{16}$

9	10	11	12	13	14	15	16
⑭	8	7	$\boxed{4}$	⑫	2	6	1

Then the subgroups are as follows:

$$\{0\} \subseteq \{1,16\} \subseteq \{1,13,16,4\} \subseteq \{1,9,13,15,16,8,4,2\} \tag{5.48}$$

Now we have the corresponding fixed fields:

$$\mathbb{Q}(\zeta), \mathbb{Q}\left(\zeta+\zeta^{16}\right), \mathbb{Q}\left(\zeta+\zeta^{13}+\cdots\right), \mathbb{Q}\left(\zeta+\zeta^{9}+\zeta^{13}+\cdots\right) \tag{5.49}$$

Notice for

$$\begin{align} \alpha &= \zeta+\zeta^{16} \tag{5.50}\\ \beta &= \zeta+\zeta^{13}+\zeta^{16}+\zeta^{4} \tag{5.51}\\ c &= \alpha+\beta = \zeta+\zeta^{13}+\zeta^{16}+\zeta^{4} \tag{5.52}\\ d &= \alpha\beta = \zeta^{3}+\zeta^{5}+\zeta^{14}+\zeta^{12} \tag{5.53} \end{align}$$

then α, β are roots of x^2+cx+d.

Remark 5.10. The previous example works for primes of the form $2n+1$. (17 corresponds to $n=8$.) So the next example is 257 and then $65,537$.[5.5]

5.9 Normal extensions and normal subgroups

Example 5.29. Consider x^4-2 over $\mathbb{Q}$. We desire to find all the subextensions. First note that the roots of this polynomial are: $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i$ which form a square in the complex plane. As a result of this, the corresponding Galois group is the group of symmetries of the square D_8. We have:

$$\left[\mathbb{Q}\left[\sqrt[4]{2}\right], \mathbb{Q}\right] = 4 \qquad \left[\mathbb{Q}\left[\sqrt[4]{2}, i\right] : \mathbb{Q}\left[\sqrt[4]{2}\right]\right] = 2 \tag{5.54}$$

[5.5] There was a rumor in the 19th century that there was a man who spent years working out these examples. . .

so the splitting field has degree 8 over $\mathbb{Q}$. Note the specific action of the two generators of D_8 is given by:

$$r\left(i\right) = i \qquad r\left(\sqrt[4]{2}\right) = i\sqrt[4]{2} \qquad s\left(i\right) = -i \qquad s\left(\sqrt[4]{2}\right) = \sqrt[4]{2} \tag{5.55}$$

Overall we have the following subgroups and intermediate fields:

$$\begin{tikzcd}
 & & \{1\} \arrow[lld, dash] \arrow[ld, dash] \arrow[d, dash] \arrow[rd, dash] \arrow[rrd, dash] & & \\
\left\langle r^2\right\rangle \arrow[d, dash] & \left\langle r^3 s\right\rangle \arrow[rd, dash] & \left\langle rs\right\rangle \arrow[d, dash] & \left\langle r^2 s\right\rangle \arrow[rd, dash] & \left\langle s\right\rangle \arrow[d, dash] \\
\left\langle r\right\rangle \arrow[rrd, dash] & & \left\langle r^2, rs\right\rangle \arrow[d, dash] & & \left\langle r^2, s\right\rangle \arrow[lld, dash] \\
 & & D_8 & &
\end{tikzcd} \tag{5.56}$$

$$\begin{tikzcd}
 & & \mathbb{Q}\left(\sqrt[4]{2}, i\right) \arrow[lld, dash] \arrow[ld, dash] \arrow[d, dash] \arrow[rd, dash] \arrow[rrd, dash] & & \\
\mathbb{Q}\left(i, \sqrt{2}\right) \arrow[d, dash] & \mathbb{Q}\left(\sqrt[4]{2}\left(1+i\right)\right) \arrow[rd, dash] & \mathbb{Q}\left(\sqrt[4]{2}\left(1-i\right)\right) \arrow[d, dash] & \mathbb{Q}\left(\sqrt[4]{2}\right) \arrow[rd, dash] & \mathbb{Q}\left(\sqrt[4]{2}i\right) \arrow[d, dash] \\
\mathbb{Q}\left(i\right) \arrow[rrd, dash] & & \mathbb{Q}\left(\sqrt{2}i\right) \arrow[d, dash] & & \mathbb{Q}\left(\sqrt{2}\right) \arrow[lld, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd} \tag{5.57}$$

Notice in this example, that the non-normal subgroups are $\left\langle r^3 s\right\rangle, \left\langle rs\right\rangle, \left\langle r^2 s\right\rangle, \left\langle s\right\rangle$ and the rest are normal. We also notice that the normal extensions of $\mathbb{Q}$ are the subextensions corresponding to the normal subgroups under the Galois correspondence. As it turns out, there is a more general statement of this.

Proposition 5.12. *Let $H \subseteq \mathrm{Gal}\left(L/K\right)$. Then H is normal iff L^K/K is a normal extension.*

Proof. We know $H \subseteq G = \mathrm{Gal}\left(L/K\right)$ is normal iff all conjugates of H under the action of G are the same as H. We also know M/K is normal iff all conjugates of M under G are the same as L. The result follows. □

Example 5.30. Let L/K be a fixed field corresponding to H such that L is normal. We seek to find $\mathrm{Gal}\left(L/K\right)$.

Warning 5.4. The tempting answer here is H. This is a standard blunder. In fact, $\mathrm{Gal}\left(M/L\right) = H$ so it is related.

We have $\mathrm{Gal}\left(L/K\right) = G/H$ which consists of the automorphisms of M fixing L. Indeed if we have $\mathrm{Aut}\left(M\right) \to \mathrm{Aut}\left(L\right)$ the kernel is the things fixing L which is H.

Proposition 5.13. *Let G be a finite group. Then there is some Galois extension L/K such that* $\operatorname{Gal}(L/K) = G$.

Proof. First take $G = S_n$, and $L = \mathbb{Q}(x_1, \cdots, x_n)$ to be the rational function on n variables. Now we let S_n act on L, and put $K = L^{S_n}$ to be the symmetric rational functions. If G is any finite group acting on any field L, then L/L^G is Galois with $\operatorname{Gal}\left(L/L^G\right) = G$ as desired. Indeed, the same works for $G \subseteq S_n$ and from Cayley's theorem, $G \subseteq \operatorname{Perm}(G)$. □

Example 5.31. Let G be a finite group. Then a harder question is whether or not there is an extension of the rationals which has Galois group G. This is in fact an open question. We do however know the answer for many particular cases.

Example 5.32. Let $G = \mathbb{Z}/5\mathbb{Z}$. Notice for $\zeta^{11} = 1$ we have that

$$\mathbb{Q}[\zeta] = (\mathbb{Z}/11\mathbb{Z})^\times = \mathbb{Z}/10\mathbb{Z} \tag{5.58}$$

has Galois group $(\mathbb{Z}/11\mathbb{Z})^\times = \mathbb{Z}/10\mathbb{Z}$ which has quotient $\mathbb{Z}/5\mathbb{Z}$. Note $\mathbb{Q}\left(\zeta + \zeta^{-1}\right) = \mathbb{Q}(\cos(2\pi/11)) = \mathbb{Q}(\zeta)^{\mathbb{Z}/2\mathbb{Z}}$. Then this has Galois group

$$(\mathbb{Z}/10\mathbb{Z}) / (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z} \tag{5.59}$$

Example 5.33. We now seek to find a non-abelian example. In particular, we take $G = S_5$. Recall $|S_5| = 120$. Consider the splitting field of $p(x) = x^5 - 4x + 2$. We notice first that p is irreducible by Eisenstein for $p = 2$. Next, notice that p has three real roots, and 2 non-real roots. Next notice that the Galois group $G \subseteq S_5$ which is the permutations of the 5 roots. We want to show they are in fact equal. Next notice that the Galois group contains a 5 cycle because $5 \mid |G|$ since the polynomial is irreducible. Therefore the splitting field has degree divisible by 5. Finally notice that G contains a transposition. In particular, we note that flipping two roots exchanges the others (just complex conjugation.) Recall that any five cycle and a transposition generate the entirety of S_5 as desired.

Proposition 5.14. *Let $p \in \mathbb{Z}$ be prime. Then we can find an extension $L/\mathbb{Q}$ such that* $\operatorname{Gal}(L/\mathbb{Q}) = S_p$.

Proof. We follow the same reasoning as in example 5.33. We just need to find an irreducible polynomial of degree p with exactly two complex roots. □

Corollary 5.2. *Let G be a finite group. We can find an extension L/K of $\mathbb{Q}$ such that* $\operatorname{Gal}(L/K) = G$.

Proof. Let L be the extension such that $\operatorname{Gal}(L/\mathbb{Q}) = S_p$ for some sufficiently large p such that $G \subseteq S_p$. Then take $K = L^G$ and the result follows. □

Remark 5.11. No one knows how to make $L^G = \mathbb{Q}$ in general.[5.6]

[5.6] This is relevant in algebraic number theory. See [4].

5.10 Applications to polynomials

Proposition 5.15. *Consider an irreducible polynomial*

$$p\left(x\right)=x^{3}+ax^{2}+bx+c=0 \tag{5.60}$$

in $K\left[x\right]$. Then the Galois group G of the splitting field is S_3 iff the discriminant of p is not a square in K. If the discriminant is a square, then the Galois group is cyclic of order 3, equal to A_3 as a permutation of the roots of f.

Proof. In any case, the Galois group $G\subseteq S_3$ which is the group of all permutations of the roots. We look at

$$\Delta=\left(\alpha-\beta\right)\left(\beta-\gamma\right)\left(\gamma-\alpha\right) \tag{5.61}$$

where α,β,γ are the roots of the polynomial. Δ is fixed by $\mathbb{Z}/2\mathbb{Z}$, but it changes sign under odd permutations of the roots. As such, if the Galois group is $\mathbb{Z}/3\mathbb{Z}$ then Δ must be in K. If $G=S_3$ then $\Delta\mapsto-\Delta$ must be an automorphism. Therefore it must be the case that the determinant Δ^2 has a square root in K. This is a symmetric function of α,β,γ and explicitly we can write it as: $\Delta^2=-4b^2-27c^2$ if $a=0$. □

Example 5.34. Consider the polynomial x^3-2 over the rationals. The Galois group of this polynomial is S_3.

Example 5.35. Consider the polynomial x^3+x+1 for the finite field with two elements: F_2. This has Galois group $\mathbb{Z}/3\mathbb{Z}$.

Example 5.36. Consider the polynomial x^3-3x-1 over the rationals. We can explicitly calculate that $\Delta^2=81$ which is a square of the rational 9, meaning the Galois group must be $\mathbb{Z}/3\mathbb{Z}$.

5.10.1 Algebraic closure of $\mathbb{C}$

Theorem 5.5. $\mathbb{C}$ *is algebraically closed.*

Proof. Recall the following facts about $\mathbb{R}$ and $\mathbb{C}$:

1. $\mathbb{R}$ has characteristic 0
2. Any odd degree polynomial in $\mathbb{R}\left[x\right]$ has a real root. (This follows from the intermediate value theorem.)
3. $[\mathbb{C}:\mathbb{R}]=2$ and every element of $\mathbb{C}$ has a square root in $\mathbb{C}$.

Let L be a finite extension of $\mathbb{C}$. Leaving L arbitrary, it is sufficient to show $L=\mathbb{C}$. We might as well extend L to a Galois extension. To see this, note that the normal closure of K over $\mathbb{R}$ still has a finite degree over $\mathbb{C}$ (or $\mathbb{R}$), so we may assume without loss of generality that K is a normal extension of $\mathbb{R}$. Therefore it is a Galois extension, since every algebraic extension of a field of characteristic 0 is separable. So we have $\mathbb{R} \subseteq \mathbb{C} \subseteq L$. Let $G = \mathrm{Gal}(L/\mathbb{R})$. We want to show that G has order 2, because this forces $L = \mathbb{C}$ as desired. Item 2 gives us that G has no subgroups of odd index greater than 1, since $\mathbb{R}$ has no extensions of odd degree. Now take any subgroup $H \subseteq \mathbb{C}$, so that H has index 2 in G. Item 3 gives us that H has no subgroups of index 2, since $\mathbb{C}$ has no subgroups of index 2.

Since 2 divides the order of G we have some 2-Sylow subgroup S of G. S has odd index, so $S = G$ by item 2. So $S = G$ has order 2^n for some n. Therefore H has order 2^{n-1}. If $n - 1 > 0$, H has subgroups of index 2, which would contradict item 3, so $|H| = 1$ and $|G| = 2$ as desired. □

Remark 5.12. The above proof is mostly algebraic, though not entirely, since we took some analytic concepts for granted. For a purely analytic proof of theorem 5.5 see a complex analysis text such as [1, 2].

5.10.2 Structure of separable extensions

Lemma 5.3. *Let V be a vector space over an infinite field K. Then V is not a union of finitely many proper subspaces of V.*

Proof. Proceed by induction. Let $V_1, \cdots, V_n$ be proper subspaces of V. Take $v \notin V_1, \cdots, V_{n-1}$ by induction and $w \notin V_n$. Then consider $u = v + kw$ for $k \in K$. Then there is at most 1 value of k for which $u \in V_i$ for any given i. Since K is infinite, we can choose k such that $v + kq$ is not in any V_j. □

Theorem 5.6. *Let L/K be a finite separable extension. Then L is generated by 1 elements. In other words there exists some $\alpha \in K$ such that $K = L(\alpha)$.*

Proof. First, we know there are only finitely many extensions between K and L. Let M be a Galois extension containing L. Then there are only finitely many extensions of K in M, since these correspond to subgroups of the Galois group. Each extension is a vector space over K. Suppose K is infinite. Then the vector space L is not a union of a finite number of subspaces, so some element $\alpha \in L$ is not in any smaller extension of K, so $L = K(\alpha)$. If K is finite, then L is finite, so $L^\times$ is cyclic. □

Example 5.37. We give an example of what it called a purely inseparable extension. These tend to be very weird and break your intuition.[5.7] Consider $F_p(t^p, u^p) \subseteq F_p(t, u)$. This has degree p^2, since

$$[F_p(t,u) : F_p(t,u^p)] = [F_p(t,u^p) : F_p(t^p,u^p)] = (p)(p) = p^2 \qquad (5.62)$$

Every element $a \in F_p(t,u)$ generates an extension of degree p or 1. In fact, $a^p \in F_p(t^p, u^p)$ for t or u. Therefore $F_p(t,u)$ is not generated by 1 element, and there are infinitely many extensions between $F_p(t^p, u^p)$ and $F_p(t,u)$.

[5.7] There is a theorem due to Jacobson showing in some cases, subfields of this nature are the same as subalgebras of Lie algebras.

5.11 Cyclic extensions

Definition 5.12. Let K be a field, and L/K be a Galois extension. L/K is a *cyclic extension* iff the $\mathrm{Gal}\,(L, K)$ is a cyclic group.

5.11.1 Prime order

Remark 5.13. We now consider what can be said about some Galois extension L/K, given that $\mathrm{Gal}\,(L, K) = \mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proposition 5.16. *Let $K = \mathbb{Q}\,(\zeta)$ where ζ is a primitive p-th root of unity. Let $L = K\,(\sqrt[p]{a})$ for some $a \in K$. Then* $\mathrm{Gal}\,(L, K) = \mathbb{Z}/p\mathbb{Z}$*.*

Proof. We know $\sqrt[p]{a}$ is a root of $x^p - a$. The other roots are $\sqrt[p]{a}$, $\sqrt[p]{a}\zeta$, $\sqrt[p]{a}\zeta^2, \cdots$. This means any element of the Galois group takes $\sqrt[p]{a}$ to $\sqrt[p]{a}\zeta^i$ for some i. Therefore the Galois group is a subgroup of $\mathbb{Z}/p\mathbb{Z}$, but since p is prime, this means it must either be the trivial group, or $\mathbb{Z}/p\mathbb{Z}$ itself. □

Proposition 5.17. *Let K contain all p-th roots of unity, and let* $\mathrm{char}\,(K) \neq p$*. Then if* $\mathrm{Gal}\,(L, K) = \mathbb{Z}/p\mathbb{Z}$ *for some extension L/K, then $L = K\,(\sqrt[p]{a})$ for some $a \in K$.*

Proof. In order to find such an a, let σ be a generator of the Galois group $\mathbb{Z}/p\mathbb{Z}$. Note $\sigma^p = 1$. The key idea here is to look at the action of σ on L viewed as a vector space over K. In this sense, σ is a linear transformation, so we can look at its eigenvalues and eigenvectors. We hope to diagonalize σ.

We know its eigenvalues are the roots of $x^p - 1$ which lie in K, since $\sigma^p = 1$. We now seek to find the corresponding eigenvectors. Choose some $v \in L$, and consider:

$$v + \sigma v + \sigma^2 v + \cdots + \sigma^{p-1} v \tag{5.63}$$

which has corresponding eigenvalue 1. Similarly, we consider:

$$v + \zeta\sigma v + \cdots + \zeta^{p-1}\sigma^{p-1} v \tag{5.64}$$

which has eigenvalue ζ^{-1}. We then get that

$$v + \zeta^{-1}\sigma v + \cdots + \zeta^{1-p}\sigma^{p-1} v \tag{5.65}$$

is an eigenvector with corresponding eigenvalue $\zeta = \zeta^{1-p}$. Notice that v is the average of these, since $v = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$. As such, L is a direct sum of p one dimensional subspaces, on which σ acts as $1, \zeta, \zeta^2, \cdots$.

Now pick w to be any eigenvector of σ with eigenvalue not equal to 1. In other words, $q \notin K$, where K is a subspace with eigenvalue 1. Then we have that $\sigma w = \zeta w$, say, which means $\sigma w^p = \zeta^p w^p = w^p$. So $w^p \in K$, since it is fixed by σ. Then we can take $a = w^p \in L$ so $L = K\,(\sqrt[p]{a})$. □

Remark 5.14. The following theorem is a summary of the above propositions, which are phrased more as one might derive the result.

Theorem 5.7. *Let L/K be a Galois extension. If the following hold:*

1. $\mathrm{Gal}\,(L, K) = \mathbb{Z}/p\mathbb{Z}$
2. *K contains roots of $1 + x + \cdots + x^{p-1}$*
3. *K has characteristic $\neq p$*

then we have that $L = K\left(\sqrt[p]{a}\right)$ for some $a \in K$.

Remark 5.15. We now consider the case when K has characteristic p.

Proposition 5.18. *Let $\mathrm{char}\,(K) = p$, and L/K be a Galois extension such that $[L : K] = p$. We have only two possibilities:*

1. *$x^p - x - b$ is irreducible, so it yields a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$.*
2. *$x^p - x - b$ factors into linear factors. Here b is of the form $c^p - c$ for $c \in K$.*

Proof. Let σ be a generator of the Galois group. We see that L cannot be of the form $K\left(\sqrt[p]{a}\right)$ as before, since $x^p - a$ is inseparable, since all the roots are the same. Therefore the splitting field is not Galois.

Again look at the eigenvalues and eigenvectors of σ on L as viewed as a vector space. Since $\sigma^p = 1$, then $(\sigma - 1)^p = 0$ so $\sigma - 1$ is nilpotent, and not diagonalizable. The only eigenvalue is 1, and the eigenspace is K. For motivation we consider the following form of a nilpotent matrix:

$$M = \begin{pmatrix} 0 & 1 & * & * \\ & 0 & 1 & * \\ & & 0 & 1 \\ & & & 0 \end{pmatrix} \tag{5.66}$$

Since it is clear the generated eigenvectors (resp. eigenvalues) are of no use, we instead consider the generalized eigenvectors (resp. eigenvalues). We first try to find the easiest generalized eigenvector: $(\sigma - 1)^2 v = 0$. This equation gives that $(\sigma - 1)\, v \in K$, since it is fixed by σ. Therefore for some $a \in K$ and $v \in$L we have that $\sigma v - v = a$. Bringing v to v/a, this gives us that $\sigma v - v = 1$. This means $\sigma v = v + a$ and $\sigma v^p = v^p + 1$. Then $\sigma\left(v^p - v\right) = v^p - v$ so $v^p - v \in K$. Therefore r is a root of $x^p - x - b$ for some $b \in K$. This is called an *Artin-Schreier* equation, and stands in as the analogue of $x^p - b$ in this scenario. Therefore $L = K\,(v)$ where v is a root of an A-S polynomial.

Let v be a root of $x^p - x - b$ in characteristic p. What are the other roots?

$$(v + a)^p - (v + 1) - b = v^p + 1 - v - 1 - b = v^p - v - b = 0 \tag{5.67}$$

which means the other roots are $v, v + 1, v + 2, \cdots, v + (p - 1)$. This give p distinct roots. This means $K\,(v)$ is separable. We also have that it is normal, because given one root, we have shown we can find the other. Therefore $K\,(v)$ is Galois, and is a subgroup of $\mathbb{Z}/p\mathbb{Z}$. □

Example 5.38. Let's apply this to the construction of finite fields. Recall the issue with p^2. We know for $F_p\left(\sqrt[p]{a}\right)$ that a is not a square in F_p. However, there is no neat way to write down a in general. We can make a choice of irreducible polynomial. What about p^p? Here we can take any root of $x^p - x - 1$, and check that this has no roots over F_p. To see this, note that $x^p - x = 0$ for all $x \in F_p$.

Example 5.39. Given a polynomial, a classical problem is to find formulas for its roots.[5.8] For example, $x^2 + bx + c$ has roots determined by the quadratic formula:

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \tag{5.68}$$

There are no formulas for 5th degree polynomials, as we will see.

5.11.2 Solvable Galois groups

Remark 5.16. So we have seen that $K\left[\sqrt[n]{a}\right]$ is a cyclic extension of K, if the characteristic does not divide n, and is $K[\alpha]$ otherwise, where $\alpha^p - \alpha - b = 0$. The novelty here, is that given one root α, we get all the others as $\alpha\zeta^i$ and $\alpha + i$ respectively.

Theorem 5.8. *The Galois group of the splitting field of a polynomial is solvable iff roots can be given using radicals and Artin-Schreier equations (*$\text{char} > 0$*).*

Proof. Let an equation be solvable by radicals. Assume the base field K contains all required roots of unity. Look at $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq L$ where L is the splitting field of the polynomial. $K_1 = K_0\left(\sqrt[n]{a_0}\right)$. Then we consider the corresponding groups:

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq 1 \tag{5.69}$$

where G_i is normal in G_{i-1} and G_{i-1}/G_i is cyclic of prime order. Look at the fields:

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq L \tag{5.70}$$

where $K_1 = L^{G_1}$ and $K_2 = L^{G_2}$. Then we have that K_{i+1}/K_i is a cyclic Galois extension, so $K_{i+1} = K_i\left(\sqrt[n]{a}\right)$ or A-S. □

Example 5.40. Consider the polynomial $x^5 - 4x + 2$. The corresponding Galois group is S_5, which has order 120. The only normal subgroups are $1, A_5, S_5$. This polynomial is therefore not solvable by radicals.

Example 5.41. The polynomial $x^5 - 2$ is irreducible and of degree 5, but it can be solved by radicals. In particular, the Galois group is solvable. The field extensions look like

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}\left(\zeta, \sqrt[5]{2}\right) \tag{5.71}$$

[5.8] Mathematicians (in particular Italian ones) used to hold duels for prestigious positions by challenging one another with difficult problems. This was a high-stakes game, because these positions often came with money and prestige. As such, when Cardano came up with a general solution for finding roots of degree 4 polynomials, this became a valuable trick of the trade.

The corresponding groups of the quotients of the Galois groups are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$, which are cyclic.

Proposition 5.19. *Let K be a field such that* $\operatorname{char}(K) = 0$*. All polynomial of degree ≤ 4 in $K[x]$ can be solved by radicals.*

Proof. The Galois group is a subgroup of S_4 so it is solvable. We have:

$$S_4 \supseteq A_4 \supseteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \supseteq 1 \tag{5.72}$$

all quotients are abelian, so S_4 is solvable since any abelian group splits into cyclic ones. This comes out of this weird S_4 coincidence where we get an extra normal subgroup. □

Example 5.42. The polynomial $x^4 + x + 1$ is hard.

5.12 Cyclotomic polynomials

5.12.1 Examples and definitions

Example 5.43. We know that over $\mathbb{Q}$, the roots of the unity are the roots of $x^n - 1$ for various n. By how does this polynomial factorize into irreducibles? Consider $x^{12} - 1$ for example. Regarding these roots as points on the unit disk, we get that $x - 1$ divides our polynomial from the point at 1, $x^2 - 1$ divides our polynomial from the point at -1, $x^4 - 1$ divides our polynomial from the point at i, $x^4 - 1$ divides our polynomial from the point at $-i$, $x^6 - 1$ divides our polynomial from the point at $-\pi/3$, etcetera. These however have common factors. We would like to extract the irreducible core from this.

Definition 5.13. The n-th *cyclotomic polynomial*, written $\Phi_n(x)$ is the polynomial with the primitive n-th roots as its roots.

Example 5.44. We compute the first few cyclotomic polynomials, both for reference and practice:

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^3 + x + 1 = \frac{x^3 - 1}{x - 1}$
4	$x^2 + 1 = \frac{x^4 - 1}{x^2 - 1}$
5	$x^4 + x^3 + x^2 + x + 1 = \frac{x^5 - 1}{x - 1}$
6	$x^2 - x + 1 = \frac{(x^6 - 1)(x - 1)}{(x^3 - 1)(x^2 - 1)}$

Example 5.45. Since we threw out the square roots of 1 twice, we add the factor of $\left(x^2-1\right)$ back in.

$$\begin{aligned}\Phi_{12}(x) &= \frac{\left(x^{12}-1\right)\left(x^2-1\right)}{\left(x^6-1\right)\left(x^4-1\right)} = x^3-x^2+1 && (5.73)\\ x^{12}-1 &= \Phi_{12}(x)\,\Phi_6(x)\,\Phi_4(x)\,\Phi_3(x)\,\Phi_2(x)\,\Phi_1(x) && (5.74)\end{aligned}$$

Example 5.46. Again, in order to make sure we're not dividing by factors twice, we add things back in to the numerator:

$$\Phi_{15}(x) = \frac{\left(x^{15}-1\right)(x-1)}{\left(x^5-1\right)\left(x^3-1\right)} = x^8-x^7+x^5-x^4+x^2-x+1 \qquad (5.75)$$

Exercise 5.12.1. Find the smallest n such that $\Phi_n(x)$ has a coefficient which is not 0 or ±1. [Hint: This happens for $n > 100$. As such, this should not be done by brute force, but rather one should calculate the first few to recognize some patterns. This will make you really understand Cyclotomic polynomials.]

Solution. It turns out that:

$$\begin{aligned}\Phi_{105}(x) &= x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39} && (5.76)\\ &\quad +x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}-x^{28}-x^{26} && (5.77)\\ &\quad -x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13} && (5.78)\\ &\quad +x^{12}-x^9-x^8-2x^7-x^6-x^5+x^2+x+1 && (5.79)\end{aligned}$$

Theorem 5.9. *$\Phi_n(x)$ is irreducible over $\mathbb{Q}$. The corresponding Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Let b be prime. We have proved this using Eisenstein's criterion. A similar proof works for prime powers. For general n, we use a different argument. The first key idea is to reduce modulo prime p. The second key idea is to use the Frobenius map: $F(t) = t^p$, where the field has characteristic p. F is an automorphism.

Let f be an irreducible factor of $\Phi_n(x)$ over $\mathbb{Q}$. Form $\mathbb{Z}[\zeta] = \mathbb{Z}[x]/f(x)$. This is an integral domain, and the quotient field $\mathbb{Q}(\zeta)$ is generated by a primitive n-th root ζ of 1. Use $\mathbb{Z}$ not $\mathbb{Q}$ to reduce modulo p. $\mathbb{Z}[\zeta]$ contains n distinct roots of x^n-1. These are $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$. Now choose an irreducible factor $g(x)$ of $f(x)$ in $F_p(x)$. In other words factor f modulo p. In general, $\deg g < \deg f$. The key point is that since x^n-1 has n distinct roots, $nx^{n-1} = \frac{d}{dx}\left(x^n-1\right)$ and x^n-1 are coprime.

Now since g is irreducible, and ζ is a root of g, then ζ^p is also a rot of g since $t \mapsto t^p$ is an automorphism of $F_p(\zeta)$. So in $\mathbb{Z}[\zeta]$, ζ^p is also a root of f. Then the map from roots of unity in $\mathbb{Z}[s]$ to roots of unity in $F_p(\zeta)$ is bijective. So if p does not divide n, then the roots of f are closed under the map $\zeta \mapsto \zeta^p$.

Now consider the Galois group of $\mathbb{Z}[\zeta]$. Automorphisms take $\zeta \mapsto \zeta^k$ for k, n coprime, so the Galois group is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. The Galois group contains $\zeta \mapsto \zeta^p$ for p, n coprime, which generate $(\mathbb{Z}/n\mathbb{Z})^\times$. So the Galois group equals $(\mathbb{Z}/n\mathbb{Z})^\times$, and $f = \Phi_n(x)$ since they have the same degree. □

Definition 5.14. A cyclotomic[5.9] field is a field generated by roots of unity.

5.12.2 Prime numbers

Theorem 5.10. *Let $n \in \mathbb{Z}$. There are infinitely many primes $p > 0$ with $p \equiv 1 \pmod{n}$.*[5.10]

Proof. The key idea is to look at the primes p which divide $\Phi_n(a)$ for some a. Let p, n be coprime. Then all of the roots of $\Phi_n(x)$ are distinct modulo p. As such, $\Phi_n(x)$ is coprime to $\Phi_m(x)$ in $F_p(x)$ as long as $m|n$. So if p divides $\Phi_n(a)$, then p does not divide $\Phi_m(a)$ for $m|n$. This says that if $\Phi_n(a) \equiv 0 \pmod{p}$, then $\Phi_m(a) \not\equiv 0 \pmod{p}$ when $m|n$. So if $a^n \equiv 1 \pmod{p}$, then $a^m \not\equiv 1 \pmod{p}$ for $m|n$. So a has order exactly n modulo p. Therefore n divides the order $(\mathbb{Z}/p\mathbb{Z})^\times$ which is $p-1$, so $p \equiv 1 \pmod{n}$.

So if $p|\Phi_n(a)$, either $p|n$, or $p \equiv 1 \pmod{n}$. Suppose $p_1, \cdots, p_k$ are $1 \pmod{n}$. Choose p dividing $\Phi_n(np_1\cdots, p_k)$. $\Phi_n(x) = 1 + x + \cdots$, so this is $1 \pmod{np_1\cdots p_k}$ and p does not divide $p_1\cdots p_k$. Then p does not divide n, so we have found p, a new prime $\equiv 1 \pmod{n}$. □

Example 5.47. Let $n = 8$. Then $\Phi_8(a) = a^4 + 1$. If $a = 1$, we get 2 which divides 8. If $a = 2$ we get 9 which is $1 \pmod{8}$. If $a = 3$, we get $82 = 41 \times 2$ and $41 \equiv 1 \pmod{8}$, and $2|8$.

5.12.3 Rational Galois extensions

Remark 5.17. We can now revisit the problem from above: given a finite group, is this group a Galois group of some extension $K/\mathbb{Q}$?

Theorem 5.11. *Let G be a finite Abelian group. Then there exists some $K/\mathbb{Q}$ such that G is the Galois group of $K/\mathbb{Q}$.*

Proof. Recall we can write G as a product of cyclic groups, since it is finite and abelian:

$$G = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \tag{5.80}$$

Choose distinct primes $p_1 \equiv 1 \pmod{n_1}, p_2 \equiv 1 \pmod{n_2}, \cdots$. Then $\mathbb{Z}/n_1\mathbb{Z}$ is a quotient of $(\mathbb{Z}/(p_1)\mathbb{Z})^\times$. As such, G is a quotient of

$$(\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots)^\times = (\mathbb{Z}/(p_1p_2\cdots)\mathbb{Z})^\times \tag{5.81}$$

which is the Galois group of $x^{p_1\cdots p_n} - 1$. Therefore any quotient G/H is the Galois group of some extension $K/\mathbb{Q}$. So if the quotient is G/H take K to be the fixed field of H so the quotient group is just the Galois group of this extension. □

Theorem 5.12 (Kronecker-Weber-Hilbert)**.** *If $K/\mathbb{Q}$ is a Galois extension with Abelian Galois group, then $K \subseteq \mathbb{Q}[\zeta]$ for ζ some root of unity.*[5.11]

[5.9] "Cyclo" means "circle," and "tomic" means "cut."

[5.10] Dirichlet proved this result for when $p \equiv a \pmod{n}$. However, the proof is not as nice. It seems that the nice proof cannot be extended to the more general case.

[5.11] For a proof see a text on algebraic number theory such as [4].

5.12.4 Finite division algebras

Remark 5.18. Can we find analogues of the quaternions $\mathbb{H}$? This is a division algebra that is a "non-commutative field".

Theorem 5.13 (Wedderburn)**.** *Any finite division algebra is a field, and is therefore commutative.*

Proof. Recall that any group G is the union of its conjugacy classes, which have sizes $|G| \,/\, |H|$, where H is a subgroup centralizing a representative element of a conjugacy class.

Now let L be a finite division algebra, and K to be its center. Also let F_q be a field of order q for some prime power q. Consider the group $G = L^\times$, which has order $q-1$. ($[L:K]=n$) Suppose $a \in G$. The centralizer of a in L is a subfield of order q^k for some k, so the centralizer of a in G is a subfield of order $q^k - 1$, to remove the element 0. So look at the class equation for G to get:

$$q^n - 1 = |G| = q - 1 + \sum_i \frac{q^n - 1}{q^{k_i - 1}} \tag{5.82}$$

where the sum runs over the conjugacy classes of orders

$$q \geq \frac{1}{q^{k_i - 1}} > 1 \tag{5.83}$$

So $q-1$ conjugacy classes of size 1. Note that $k_i < n$. This is a subtle but key point.

Now we look at the cyclotomic polynomials. We notice that q^{n-1} is divisible by $\Phi_n(q)$. Also note that so is $(q^n - 1) \,/\, \left(q^{k_i - 1}\right)$ since $k_i < n$. So $q-1$ is divisible by

$$\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(q - \zeta^i\right) \tag{5.84}$$

However, we now observe that $|q - \zeta_i| > q-1$ unless $\zeta^i = 1$ which means $L = K$, and L is therefore commutative. □

Definition 5.15 (Brauer group)**.** The Brauer group is the group of isomorphism classes of a finite dimensional division algebra over a field K with center K.

Example 5.48. The Brauer group of $\mathbb{R}$ has 2 elements: $\mathbb{R}$ and $\mathbb{H}$.

Proposition 5.20. *If D_1, D_2 are division algebras, $D_1 \otimes_K D_2 \cong M_n(D_3)$ for some n, D_3 where D_3 is the product of D_1, D_2 in the Brauer group.*

Remark 5.19. Wedderburn's theorem shows that the Brauer group of a finite field is trivial.

5.13 Norm and trace

5.13.1 Definitions and basic properties

Definition 5.16. Let L/K be a finite extension. Taking $a \in L$, then the *trace* of a is its trace when viewed as a linear transformation from $L \to L$ where L/K is viewed as a vector space over K. The *norm* of $a \in L$, written $N_{L/K}(a)$ is the determinant of a as a linear transformation in the same sense as before.

Example 5.49. Take the extension $\mathbb{C}/\mathbb{R}$ and $a = x + iy \in \mathbb{C}$. A basis for $\mathbb{C}/\mathbb{R}$ is $\{1, i\}$. We have $a \cdot 1 = x + iy$ and $a \cdot i = -y + ix$ which determined the action of a. So a can be given the matrix representation:

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \tag{5.85}$$

Therefore the trace of a is $2\operatorname{Re}(a) = 2x$ and the norm is $|a|^2 = x^2 + y^2$.

Remark 5.20. As motivated by the last example, the norm and trace can be viewed as a generalization of the modulus squared and the real part of an element of an extension.

Proposition 5.21. *Let $a, b \in L/K$ be elements of finite extension. Then*

$$N_{L/K}(ab) = N_{L/K}(a)\,N_{L/K}(b) \qquad\qquad \operatorname{Tr}(a+b) = \operatorname{Tr}(a) + \operatorname{Tr}(b) \tag{5.86}$$

Proof. This follows directly from the corresponding statements for matrices. □

Remark 5.21. Note that the norm is a homomorphism from $L^{\times}$ to $K^{\times}$ under $\times$, and the trace is a homomorphism from $L \to K$ under $+$.

Remark 5.22. Now we want to see if we generate an extension with some element, we can express the trace and norm of that element in terms of its irreducible polynomial.

Proposition 5.22. *Let $L = K[a]$ be an extension L/K generated by a. Then a satisfies some irreducible polynomial*

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0 \tag{5.87}$$

Denote the roots of this polynomial by $a_1, \cdots, a_n$. Then we have that

$$\operatorname{Tr}(a) = -b_{n-1} = \sum_{i=1}^{n} a_i \qquad\qquad N(a) = \pm b_0 = \prod_{i=1}^{n} a_i \tag{5.88}$$

Proof. First we choose a basis for L over K. The obvious choice is $\left\{1, a, a^2, \cdots, a^{n-1}\right\}$. Then it is easy to see that the action of a is

$$1 \xrightarrow{\times a} a \xrightarrow{\times a} a^2 \xrightarrow{\times a} \cdots \xrightarrow{\times a} a^{n-1} \xrightarrow{\times a} \left(-b_{n-1}a^{n-1} - b_{n-2}a^{n-2} - \cdots - b_0\right) \tag{5.89}$$

so the matrix which acts as the linear transformation given by a can be written:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ -b_0 & \cdots & \cdots & \cdots & -b_{n-2} & -b_{n-1} \end{pmatrix} \tag{5.90}$$

Which clearly has trace of $-b_{n-1}$ and determinant of $\pm b_0$. Now call the roots of the irreducible polynomial satisfied by a: $a_1, \cdots, a_n$. Then $b_{n-1} = a_1 + \cdots + a_n$ and $b_0 = \pm a_1 \cdots a_n$. □

Example 5.50. Take $\mathbb{C}/\mathbb{R}$ again to see that indeed $\operatorname{tr}(z) = z + \bar{z}$ and $N(z) = z\bar{z}$.

Remark 5.23. We now seek to show a similar result for the general case where the extension is not only generated by a single element.

Theorem 5.14. *Suppose $K \subseteq K[a] \subseteq L$. Then $N_L(a)$ is the product of all roots of irreducible polynomial of a, where we count each root $[L : K[a]]$ times. Likewise for* $\operatorname{tr}(a)$.

Proof. It follows from the above properties of the norm and trace that we have

$$N_L(a) = \left(N_{K[a]}(a)\right)^{[L:K[a]]} \qquad \operatorname{tr}_L(a) = \left(\operatorname{tr}_{K[a]}(a)\right) \times [L : K[a]] \tag{5.91}$$

The rest is left as an exercise. □

Proposition 5.23. *Let L/K be a Galois extension, and call $G = \operatorname{Gal}(L/K)$. Then*

$$N(a) = \prod_{\sigma \in G} \sigma(a) \qquad \operatorname{tr}(a) = \sum_{\sigma \in G} \sigma(a) \tag{5.92}$$

Proof. If a is some root, then the other roots are given by $\sigma_i(a)$ for $\sigma_i \in G$. The result follows. □

5.13.2 Algebraic integers

Example 5.51. Recall that in $\mathbb{Q}\left(\sqrt{-3}\right)$ we have $\mathbb{Z}\left(\sqrt{-3}\right) \subseteq \mathbb{Q}\left(\sqrt{-3}\right)$. But $\mathbb{Z}\left(\sqrt{-3}\right)$ is not a UFD. To see this we can simply consider that

$$4 = 2 \times 2 = \left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right) \tag{5.93}$$

However, the field $\mathbb{Q}\left[\left(\sqrt{-3} + 1\right)/2\right]$ is a UFD.

Remark 5.24. As motivated by the previous example, we might wonder if given a field $L \supseteq \mathbb{Q}$, is there is a nice ring inside of L? This is the motivating notion behind the algebraic integers.

Definition 5.17. The algebraic integers of a field K are the roots of polynomials in $\mathbb{Z}[x]$ with leading coefficient 1.

Example 5.52. For example, the polynomial $x^2+x+1=0$ has leading coefficient 1, and $w=\left(\sqrt{-3}+2\right)/2$ certainly is a root.

Remark 5.25. But why does a leading coefficient of 1 make things behave?

Theorem 5.15. *Let $L/\mathbb{Q}$ be a finite extension. Then for $\alpha\in L$, TFAE:*

1. *α is an algebraic integer (root of $x^n+\cdots=0$.)*
2. *There exists some finitely generated $\mathbb{Z}$ module A in L spanning L, so that $\alpha A\subseteq A$.*

Proof. (1) $\Longrightarrow$ (2): Take A spanned by $\left\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\right\}$. Then $\alpha\alpha^{n-1}$ is a linear combination of the elements of the spanning set.

(2) $\Longrightarrow$ (1): Think of α as a linear transformation of the free $\mathbb{Z}$-module A. Then α is a root of its characteristic polynomial, which has leading coefficient 1, and the remaining coefficients in $\mathbb{Z}$. □

Proposition 5.24. *The algebraic integers form a subring.*

Proof. See a text in algebraic number theory such as [4]. □

Remark 5.26. We now wish to see how one can find an algebraic integer in a quadratic field.

Proposition 5.25. *If α is an algebraic integer of some field K, then we have that* $\operatorname{tr}(\alpha)$ *and $N(\alpha)$ are also algebraic integers.*

Proof. This is a consequence of the fact that the conjugate of α is also algebraic, and the sum of product of algebraic integers is still algebraic. □

Proposition 5.26. *Let $L=\mathbb{Q}\left[\sqrt{N}\right]$ where $N\in\mathbb{Z}$ is square free.*[5.12] *Then the algebraic integers are:*

$$\mathbb{Z}\left[\sqrt{N}\right] \quad \text{if} \quad N\equiv 2,3 \pmod 4 \tag{5.94}$$

$$\mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] \quad \text{if} \quad N\equiv 1 \pmod 4 \tag{5.95}$$

Proof. We seek to find the algebraic integers in L. There are some obvious examples: $m+n\sqrt{N}$ for $m,n\in\mathbb{Z}$. However, there are sometimes others. We saw this in the case of $\left(\sqrt{3}+1\right)/2$. The key point here is that for some algebraic integer α, $\operatorname{tr}(\alpha)$ and $N(\alpha)$ are integers, by the previous proposition, and the fact that the only algebraic integers in $\mathbb{Q}$ are the actual integers. Then what is the norm and trace of $m+n\sqrt{N}$?

[5.12] We take this for simplicity, for if N was a square, then take out the square factor, and we are still fine.

We choose a basis first. Take $1, \sqrt{N}$ for $L/\mathbb{Q}$. Then we have

$$\begin{aligned} \times m: \quad 1 &\mapsto m \tag{5.96}\\ \sqrt{n} &\mapsto m\sqrt{n} \tag{5.97}\\ \times n\sqrt{n}: \quad 1 &\mapsto n\sqrt{N} \tag{5.98}\\ \sqrt{N} &\mapsto nN \tag{5.99} \end{aligned}$$

Then this means $m + n\sqrt{N}$ gets a matrix representation:

$$\begin{pmatrix} m & n \\ nN & m \end{pmatrix} \tag{5.100}$$

So now we can just read off that the trace is $2m$, and the norm is $m^2 - n^2$. Now since these are both integers, then either $m \in \mathbb{Z}$ or $m \in \mathbb{Z} + 1/2$. First take the case that $m \in \mathbb{Z}$. Additionally, if $m^2 - n^2N \in \mathbb{Z}$, then $n \in \mathbb{Z}$ since N is square free. then since $m, n \in \mathbb{Z}$ we just get $m + n\sqrt{N}$ for our algebraic integers. On the other hand, if $m \notin \mathbb{Z}$ things are a bit trickier. Again we have $m^2 - n^2N \in \mathbb{Z}$, and $m^2 \in \mathbb{Z} + 1/4$ so find $1/4 - n^2N \in \mathbb{Z}$ which means $1 \equiv (2n)^2 N \pmod 4$. If $N \equiv 2 \pmod 4$ or $N \equiv 3 \pmod 4$ then there are no solutions. If however $N \equiv 1 \pmod 4$ then there are solutions, since $2n$ can be odd. □

Example 5.53. The motivating example of $\mathbb{Q}\left[\left(\sqrt{-3}+1\right)/2\right]$ does indeed satisfy the previous theorem for values $N = -3, 5$.

5.13.3 Trace as a bilinear form

Proposition 5.27. *Let L/K be a field extension. Then* tr *gives a bilinear form $(\cdot,\cdot)$ where*

$$(a, b) = \operatorname{tr}(ab) \tag{5.101}$$

for all $a, b \in L$.

Proof. If $\operatorname{tr}(a) = 0$ for all a, then it is identically 0. If $\operatorname{tr}(a) \neq 0$ for some a, then this bilinear form is non-degenerate. □

Example 5.54. We seek to show when the bilinear form given by tr is identically zero for some extension L/K. In particular take $K = F_p(t^p)$ and $L = F_p(t)$. Then as we have seen $[L : K] = p$. Any $x \in L$ is a root of an equation of the form $x^p - a$ for $a \in K$. Then the coefficient of $x^{p-1} = 0$ which is the trace. Therefore the trace is identically 0, and the bilinear form is degenerate. Recall that this is the standard example of an inseparable extension. We now seek to generalize this.

Theorem 5.16. *If L/K is a separable extension, then the bilinear form given by $\operatorname{tr}_{L/K}$ is non-degenerate.*

Remark 5.27. this is obvious for char $= 0$(see beginning of proof) but otherwise we need a lemma first.

Definition 5.18. Let G be a group, K a field. The characters of G are homomorphisms from G to $K^{\times}$.

Remark 5.28. We can think of this as a one dimensional representation of G.

Lemma 5.4 (Artin)**.** *Let G be a group. If $\chi_1, \cdots, \chi_n$ are distinct characters of G, they are linearly independent. In other words, if*

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0 \tag{5.102}$$

for all $g \in G$, then it must be the case that $a_1 = \cdots = a_n = 0$.

Proof. Let G, $a_1, \cdots, a_n$ and $\chi_1, \cdots, \chi_n$ be as in the statement of the lemma. Proceed by contradiction. Suppose $a_i \neq 0$ for all i, and n is a minimal such n. Since the characters are distinct, we can find $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Then

$$a_1\chi_1(gh) + a_1\chi_2(gh) + \cdots + a_n\chi_n(gh) = 0 \tag{5.103}$$

for all g, but this can also be written:

$$\begin{aligned} 0 &= a_1\chi_1(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_n(h) && (5.104)\\ &= a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_n(h) && (5.105)\end{aligned}$$

so we can subtract to get

$$a_2(\chi_1(h) - \chi_2(h))\chi_2(g) + a_3(\chi_1(h) - \chi_3(h))\chi_3(g) + \cdots = 0 \tag{5.106}$$

but this means we have a smaller linear equation in $\chi_1, \cdots, \chi_n$ which equals 0 which is a contradiction to n being minimal. □

Proof of theorem 5.16. Let us first show this for Galois extensions. We want to show that tr is not identically 0 for a Galois extension L/K. Let $\{\sigma_i\}_{i=1}^n \subseteq \mathrm{Gal}(L/K) = G$. Then we can write

$$\mathrm{tr}(a) = \sigma_1(a) + \cdots + \sigma_n(a) \tag{5.107}$$

for any $a \in L$. Now if $\mathrm{tr}(a) = 0$ for all $a \in L$ then there is some linear relation between $\sigma_1, \cdots, \sigma_n$ which equals 0. But by Artin's lemma, this cannot be possible unless each coefficient is 0. Therefore there exists some $a \in L$ such that $\mathrm{tr}(a) \neq 0$. We leave the generalization to separable extensions as an exercise. In short, instead of summing over elements of G we sum over coset representatives. □

5.13.4 Discriminants of field extensions

Definition 5.19. Let L/K be a field extension, and $\{a_i\}_{i=1}^n$ a basis for L over K. Then The discriminant of the extension is the discriminant of the bilinear form given by the corresponding trace. In other words, it is

$$\det\begin{pmatrix}(a_1,a_1) & (a_1,a_2) & \cdots & (a_1,a_n)\\ (a_2,a_1) & (a_2,a_2) & \cdots & (a_2,a_n)\\ \vdots & \vdots & \vdots & \vdots\\ (a_n,a_1) & (a_n,a_2) & \cdots & (a_n,a_n)\end{pmatrix} \tag{5.108}$$

Remark 5.29. The notion of the discriminant of a field extension is only valid up to multiplication by squares of our base field K. This is a result of a possible change of basis. In particular, if we have another basis $\{b_i\}_{i=1}^n$ then we have some matrix A which gives us a change of basis from $\{a_i\}$ to $\{b_i\}$. But then we have that the discriminant in the new basis is the same as before, only now multiplied by a factor of $\det(A)^2$. As such, the discriminant is not an element of K, but rather an element of $K^\times/\left(K^\times\right)^2$ where

$$\left(K^\times\right)^2 = \left\{a^2 \mid a \in K^\times\right\} \tag{5.109}$$

Example 5.55. Let $L = K[a]$ be a Galois extension of a field K, where a is the root of an irreducible polynomial p. We wish to find the discriminant of this extension in terms of p. Choose a basis $\left\{1, a, a^2, \cdots, a^{n-1}\right\}$ of L/K. Then the discriminant is

$$\det\begin{pmatrix} \operatorname{tr}(1) & \operatorname{tr}(a) & \operatorname{tr}\left(a^2\right) & \cdots & \operatorname{tr}\left(a^{n-1}\right) \\ \operatorname{tr}(a) & \operatorname{tr}\left(a^2\right) & \operatorname{tr}\left(a^3\right) & \cdots & \operatorname{tr}\left(a^n\right) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \operatorname{tr}\left(a^{n-1}\right) & \operatorname{tr}\left(a^n\right) & \operatorname{tr}\left(a^{n+1}\right) & \cdots & \operatorname{tr}\left(a^{2n-2}\right) \end{pmatrix} \tag{5.110}$$

Now call $G = \operatorname{Gal}(L/K)$. We know

$$\operatorname{tr}\left(\sigma^k\right) = \sum_{\sigma\in G} \sigma\left(a^k\right) \tag{5.111}$$

so the discriminant can be rewritten

$$\text{discr} = \begin{pmatrix} \sum\sigma(1\cdot 1) & \sum\sigma(a\cdot 1) & \cdots & \sum\sigma\left(a^{n-1}\cdot 1\right) \\ \sum\sigma(1\cdot a) & \sum\sigma(a\cdot a) & \cdots & \sum\sigma\left(a^n\cdot a\right) \\ \vdots & \vdots & \vdots & \vdots \\ \sum\sigma\left(1\cdot a^{n-1}\right) & \sum\sigma\left(a\cdot a^{n-1}\right) & \cdots & \sum\sigma\left(a^{n-1}\cdot a^{n-1}\right) \end{pmatrix} \tag{5.112}$$

$$= \begin{pmatrix} \sigma_1 1 & \sigma_2 1 & \cdots & \sigma_{n-1}1 \\ \sigma_1 a & \sigma_2 a & \cdots & \sigma_{n-1}a \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1 a^{n-1} & \sigma_2 a^{n-1} & \cdots & \sigma_{n-1}a^{n-1} \end{pmatrix} \tag{5.113}$$

$$\times \begin{pmatrix} \sigma_1 1 & \sigma_1 a & \cdots & \sigma_1 a^{n-1} \\ \sigma_2 1 & \sigma_2 a & \cdots & \sigma_2 a^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_{n-1}1 & \sigma_{n-1}a & \cdots & \sigma_{n-1}a^{n-1} \end{pmatrix} \tag{5.114}$$

these matrices are transposes of one another, so the discriminant is the square of the determinant of the second matrix. To find this determinant we recall the

Vandermonde determinant:

$$\det\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ a & b & c & d & e \\ a^2 & b^2 & c^2 & d^2 & e^2 \\ & & \cdots & & \\ a^{n-1} & b^{n-1} & c^{n-1} & d^{n-1} & e^{n-1} \end{pmatrix} = \pm\left(a-b\right)\left(a-c\right)\cdots\left(b-c\right)\left(b-a\right)\cdots \tag{5.115}$$

this is somewhat obvious because it must be divisible by $(a-b)$ since if $a=b$ the first two rows are identical. Then both have degree $n\left(n-1\right)/2$ so they must be the same up to a constant.

Returning to the actual problem, we have that

$$\text{discr} = \left(\det\right)^2 = \left(\pm\prod_{i<j}\left(\sigma_i a - \sigma_j a\right)\right)^2 = \Delta^2 \tag{5.116}$$

then since Δ^2 is the discriminant of the polynomial, the discriminant of $L\left[a\right]/K$ is the discriminant of p.[5.13]

Example 5.56. Consider the following fields:

field	discriminant
$\mathbb{Q}\left[x\right]/\left(x^3+x+1\right)$	-31
$\mathbb{Q}\left[x\right]/\left(x^3+x-1\right)$	-31
$\mathbb{Q}\left[x\right]/\left(x^3-x+1\right)$	-23

Where the values of the discriminants are in $\mathbb{Q}^\times/\left(\mathbb{Q}^\times\right)^2$. Then the bottom field is different from the others, since $\left(-23\right)/\left(-31\right)$ is not a square in $\mathbb{Q}^\times$. The other two have the same discriminant, and in fact form isomorphic fields.

Example 5.57. We desire to find the algebraic integers in $L = \mathbb{Q}\left[\alpha\right]$ where $\alpha^3+\alpha+1=0$. This is usually a difficult thing to do, but this particular example is relatively easy. Look at the discriminant of the basis $\{1,\alpha,\cdots\}$ which is -31.

As such, the basis consists of algebraic integers. Now suppose there are more algebraic integers in the ring. Let A be an integer linear span of our basis, and B consist of all the algebraic integers. Then we know already that $A\subseteq B$. In addition to this, we know that $\text{discr}\left(A\right) = \text{discr}\left(B\right)\times\det\left(X\right)^2$ where X brings the basis of A to the basis of B. In particular, the determinant of $X = \left[B:A\right]$. But $\text{discr}\left(A\right) = -31$ which is square free, meaning X is an integer matrix, and $\det\left(X\right)^2$ is the square of an integer. But -31 is square free, so $\det\left(X\right)^2 = 1$,

[5.13] There is a textbook called linear algebra done right, which completely avoids calculating a determinant until the end. The author boasts about this, but things like the preceding calculation are made very difficult without determinants.

and $A = B$ as desired. This shows us how a square free discriminant is quite lucky.

Example 5.58. Look at $\mathbb{Q}[\alpha]$ where $\alpha = \sqrt{-3}$. Then $\operatorname{discr}\alpha = -4 \times 3 = -12$ since $\alpha^2 + 3 = 0$. Now this is not square free, so we have that

$$\mathbb{Z}[\alpha] \subsetneq \mathbb{Z}\left[\frac{\sqrt{-3}+1}{2}\right] \tag{5.117}$$

of index 2, which gives us that

$$\operatorname{discr}\mathbb{Z}\left[\frac{\sqrt{-3}+1}{2}\right] = -3 \tag{5.118}$$

This agrees with the fact that $\operatorname{discr}\left(x^2+x+1\right) = -3$.

5.13.5 Properties of the norm

Recall that the norm is a homomorphism from $L^\times \xrightarrow{N} K^\times$ This means we can use it to compare these two fields, given an understanding of $K^\times$. This motivates the question of finding $\operatorname{im}(N)$ and $\ker(N)$.

Example 5.59. Take $\mathbb{C}/\mathbb{R}$. Then N acts by taking $x \mapsto N(z) = z\bar{z} = |z|^2$ so $\operatorname{im}(N) = \mathbb{R}^+$. As such, $\mathbb{R}^\times/N\mathbb{C}^\times$ has order 2.

Example 5.60. Consider $\mathbb{Q}[i]$ Then $\mathbb{Q}[i]^\times \xrightarrow{N} \mathbb{Q}^\times$ where $a + bi \mapsto a^2 + b^2$. Therefore we have

$$\operatorname{im}(N) = \left\{q \in \mathbb{Q} : \exists a, b \in \mathbb{Z} \,|\, a^2 + b^2 = q\right\} \tag{5.119}$$

but when can q be expressed as two squares? This is obviously a complicated question, and things only get worse at higher degrees.

Theorem 5.17. *Let L/K be a finite extension of a finite field. Then $N : L^\times \to N^\times$ is onto.*

Proof. Recall that $G = \operatorname{Gal}(L/K)$ is cyclic, and generated by the Frobenius element $F : x \to x^q$ for $q = |K|$. Then we have

$$N(a) = a \cdot Fa \cdot F^2a \cdots F^{n-1}a \tag{5.120}$$

since

$$G = \left\{1, F, F^2, \cdots, F^{n-1}\right\} \tag{5.121}$$

where $n = [L : K]$. Then we can write that

$$\begin{aligned} N(a) &= aa^qa^{q^2}\cdots a^{q^{n-1}} &(5.122)\\ &= a^{q^{n-1}+q^{n-2}+\ldots+1} = a^{\frac{q^n-1}{q-1}} &(5.123)\end{aligned}$$

Therefore there are at most $(q^n - 1)/(q-1)$ elements of norm 1, since $N(a) = 1$ has at most this many roots. But we also know that:

$$|\ker(N)| \times |\mathrm{im}(N)| = \left|L^\times\right| \tag{5.124}$$

Therefore since the order of the image is at most $q-1$, and the order of $L^\times$ is $q^n - 1$, these are in fact equalities, and N is onto as desired. □

Remark 5.30. Clearly the previous proof only works for finite fields, since we used a finite counting argument.

5.13.6 Hilbert's theorem 90

Theorem 5.18 (Hilbert's theorem 90)**.** *Let L/K be a cyclic Galois extension, and let σ generate $G = \mathrm{Gal}(L/K)$. Then $N(a) = 1$ for $a \in L$ iff there is some $b \in L^\times$ such that $a = b/\sigma b$.*

[5.14]

Proof. ($\Longleftarrow$) : If $a = b/\sigma b$ for some $b \in L^\times$, it is trivial to show that $N(a) = 1$.

($\Longrightarrow$): This direction is more difficult. This is equivalent to solving $a\sigma b = b$ for $b \neq 0$. We can think of $a\sigma$ as a linear transformation on the vector space L. Then we want to find some nonzero b which is fixed by this transformation. Well we know how to do this for finite order. Notice $(a\sigma)^2 = a\sigma a\sigma$ so this takes

$$b \mapsto a\sigma(a\sigma(b)) = a\sigma(a)\sigma^2(b) \tag{5.125}$$

so $(a\sigma)^2 = a\sigma(a)\sigma^2$. Similarly we can write

$$\begin{aligned}
(a\sigma)^3 &= a\sigma(a\sigma(a)) = a \cdot \sigma(a) \cdot \sigma^2(a) \cdot \sigma^3 && (5.126)\\
&\cdots && (5.127)\\
(a\sigma)^2 &= \underbrace{a \cdot \sigma(a) \cdot \cdots \cdot \sigma^{n-1}(a)}_{=N(a)=1} \cdot \underbrace{\sigma^n}_{=1} && (5.128)
\end{aligned}$$

which means $(a\sigma)^n = 1$. Now this makes it easy to find a fixed vector. We know a fixed point of any group G can be given by

$$\sum_{g \in G} g(v) \tag{5.129}$$

for arbitrary v. Then it is reasonable for us to claim that

$$b = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} (a\sigma)^i(\theta) \tag{5.130}$$

[5.14] The name of this theorem comes from Hilbert's "Zahlbericht" or "number report" in 1897. This collection of results concerning algebraic number theory happened to include this theorem as the 90th result.

for any $\theta \in L$. But is this b indeed what we are looking for? It is clearly fixed by $a\sigma$, and therefore gives us what we want, but this doesn't mean much if $b = 0$. Indeed, we need to divide by b, and therefore we need to take θ such that $b \neq 0$. To see what this means exactly, write our b explicitly:

$$\begin{aligned} b &= \theta + a\sigma(\theta) + \cdots + (a\sigma)^{n-1}(\theta) && (5.131)\\ &= \theta + a\sigma\theta + a\sigma(a)\sigma^2(\theta) + a\sigma(a)\sigma^2(a)\sigma^3(\theta) + \cdots && (5.132)\\ &= \left(a_0\sigma^0 + a_1\sigma^1 + \cdots a_{n-1}\sigma^{n-1}\right)\theta && (5.133)\end{aligned}$$

where $a_2 = a\sigma(a)$ etc.[5.15] Now apply Artin's lemma 5.4 on linear transformations to get that $\sigma^0, \sigma^1, \cdots, \sigma^{n-1}$ are linearly independent. In other words, for any such $a_0, \cdots, a_{n-1}$ not all 0, there is some θ such that the sum is non-zero, and therefore $b \neq 0$ as desired. □

Example 5.61. We now offer a simple application of theorem 5.18. Let K contain a primitive nth root of unity ζ where $n = [L : K]$. Then take $a = \zeta$. We can write $N(a) = \zeta \cdots \zeta = \zeta^n = 1$ so by theorem 5.18 we have that there is some b such that $\zeta = b/\sigma b$. But this means $\sigma b = \zeta b$ so $\sigma b^n = b^n$ and $L = K\left[\sqrt[n]{\bullet}\right]$. We have seen this example before, so we can view this theorem as somehow generalizing this notion to general extensions.

Remark 5.31. We will later generalize this result to generic galois extensions. In particular, the statement will be that $H^n(L^\times) = 0$ for L/K cyclic, where H^n is the tate cohomology group.

5.14 Solving equations

5.14.1 Cubic equation

Example 5.62. Let's solve $x^3 + x + 1 = 0$ using radicals. This is a sort of reality check as to see if we are actually building tools which can solve problems. First notice this polynomial is irreducible. We work out the discriminant of this polynomial. We know the general form is $-4b^3 - 27c^2$ which evaluates to -31 in this case. This is square-free, so we know the Galois group of the splitting field over $\mathbb{Q}$ is S_3. We don't want to actually work over $\mathbb{Q}$, since we want some roots of unity thrown in. Therefore we take $\mathbb{Q}(\omega)$ instead, where $\omega^3 = 1$. Explicitly, $\omega = \left(\sqrt{-3} - 1\right)/2$.

Now look at the Galois group S_3. This group is solvable, since we have

$$1 \subseteq \mathbb{Z}/3\mathbb{Z} \subseteq S_3 \qquad (5.134)$$

where $\mathbb{Z}/3\mathbb{Z}$ is normal in S_3 with quotient $\mathbb{Z}/2\mathbb{Z}$. This essentially just means we can break S_3 into two cyclic groups, one of order 2, and one of order 3. Now

[5.15] In Lang [5] this relation is just pulled out of a hat without any sort of motivation. Professor Borcherds said this was a sort of "deus ex machina" in the sense that he just sort of offered the solution up as if given to him by god.

under the Galois correspondence we have the diagrams:

$$\begin{tikzcd} L \arrow[d, dash, "3"] & 1 \arrow[d, dash, "3"] \\ K \arrow[d, dash, "2"] & \mathbb{Z}/3\mathbb{Z} \arrow[d, dash, "2"] \\ \mathbb{Q}\left[\omega\right] & S_3 \end{tikzcd} \tag{5.135}$$

We first want to find K. We know it is an extension of degree 2, and a subfield of L fixed by $\mathbb{Z}/3\mathbb{Z}$. Furthermore L is generated by the roots of our polynomial: $\alpha_1, \alpha_2, \alpha_3$. Since S_3 acts on these roots, take σ to be the generator. Then σ has the following action:

$$\sigma : \begin{tikzcd} \alpha_1 \arrow[r] & \alpha_2 \arrow[r] & \alpha_3 \arrow[ll, bend left] \end{tikzcd} \tag{5.136}$$

so K is generated by some α such that $\sigma\alpha = \alpha$, yet the elements of S_3 not in $\mathbb{Z}/3\mathbb{Z}$ take $\alpha \mapsto -\alpha$ (say). Let's try

$$\alpha = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \tag{5.137}$$

Since we can recognize the question as finding a polynomial in $\alpha_1, \alpha_2, \alpha_3$ fixed by $\mathbb{Z}/3\mathbb{Z}$, this option is effectively the simplest such polynomial. Notice that α^2 is symmetric under any changes of the α_i, so α^2 is in the base field. This means α^2 is the discriminant of $x^2 + x + 1$, so $\alpha^2 = -31$, so $K = \mathbb{Q}\left[\omega\right]\left[\sqrt{-31}\right]$.

Next we need to find L in terms of K. We know L/K is cyclic, and K contains cube roots of unity. Therefore by Hilbert's theorem 90, theorem 5.18, we have that $L = K\left[\sqrt[3]{\bullet}\right]$. But what is $\bullet$? This is the eigenvector of σ corresponding to the eigenvalue ω. But how do we find it? Let's try something of the form

$$c + \omega^{-1}\sigma(c) + \omega^{-2}\sigma^2(c) \tag{5.138}$$

This will have eigenvalue ω for any c. In particular, no one is stopping us from taking $c = \alpha_1$. We are trying to find it after all. Then we can look at

$$y = \alpha_1 + \omega^2\alpha_2 + \omega^2\alpha_3 \tag{5.139}$$

where $\alpha_2 = \sigma(\alpha_1)$ and $\alpha_3 = \sigma^2(\alpha_1)$ by the definition of σ. Then y has eigenvalue ω as desired. Then we can look at

$$z = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \tag{5.140}$$

which has eigenvalue ω^2. Now in general we also consider $\alpha_1+\alpha_2+\alpha_3$ which has eigenvalue 1, but this is 0 for our polynomial anyway, which just reduces some of our work. But now this means, if we can fine $y, z, 0$ we can find $\alpha_1, \alpha_2, \alpha_3$ just by linear algebra. Indeed, we know $y^3, z^3 \in K$ since they are fixed by σ, so we just have to work out what they are. Now after some messy algebra, where we expand these as polynomials in $\alpha_1, \alpha_2, \alpha_3$, we have

$$y^3 + z^3 = -27c = -27 \qquad y^3b^3 = -27b^3 = -27 \tag{5.141}$$

since $c = b = 1$ here. Now we notice that this means y^3, z^3 are roots of the polynomial $x^2 + 27x - 27 = 0$, so they are given by

$$\frac{27}{2} \pm \frac{3\sqrt{3}i}{2}\sqrt{-31} \tag{5.142}$$

then numerically $y \approx -3.04$ and $z \approx 0.99$. Then $\alpha_1 = (y + z)/3 \approx -0.68$. We get these numerical approximations as to assure we aren't making sign errors or the like.

Remark 5.32. A key point to notice is that since S_3 is solvable, we could reduce the cubic to a quadratic.

5.14.2 Quartic equation

Example 5.63. We now sketch how to solve a quartic equation. We follow a similar procedure as in the cubic case. Take some degree 4 polynomial: $x^4 + bx^2 + cx + d$. We want to solve this with radicals. Look at the Galois group of the splitting field over the rationals. This is S_4, which is solvable:

$$1 \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq A_4 \subseteq S_4 \tag{5.143}$$

where the quotient of the first inclusion is $(\mathbb{Z}/2\mathbb{Z})^2$, the quotient of the second inclusion is $\mathbb{Z}/3\mathbb{Z}$, and the third gives $\mathbb{Z}/3\mathbb{Z}$. Then we have the following diagrams:

$$\begin{tikzcd}
M \arrow[d, dash, "2^2"] & 1 \arrow[d, dash] \\
L \arrow[d, dash, "3"] & (\mathbb{Z}/2\mathbb{Z})^2 \arrow[d, dash] \\
K \arrow[d, dash, "2"] & A_4 \arrow[d, dash] \\
\mathbb{Q}[\omega, i] & S_4
\end{tikzcd} \tag{5.144}$$

This shows us that you get K by adjoining the square root of something, you get L by adjoining the cube root of something, and you get M by adjoining two square roots of something. Then we can use these specific groups to determine what should be adjoined at each step.

In particular, suppose $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are the roots of our polynomial. Then note that $\sum_i \alpha_i = 0$. What is L? We know it is generated by things fixed under $(\mathbb{Z}/2\mathbb{Z})^2$, which has four elements:

$$(1)(2)(3)(4) \qquad (12)(34) \qquad (13)(24) \qquad (14)(23) \tag{5.145}$$

the first of which fixes everything. Then we are trying to find polynomials in α_i which are fixed by all such permutations. Let's try:

$$y_1 = \frac{(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2}{4} = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \tag{5.146}$$

then we also look at the conjugates:

$$y_2 = \frac{\left(\alpha_1 + \alpha_3 - \alpha_2 - \alpha_4\right)^2}{4} \qquad y_3 = \frac{\left(\alpha_1 + \alpha_4 - \alpha_2 - \alpha_3\right)^2}{4} \tag{5.147}$$

so if we can find y_1, y_2, y_3 we have the roots, since we just have to take some square roots, and do some linear algebra. Notice that y_1, y_2, y_3 generate a degree 6 extension of $\mathbb{Q}\left[i, \omega\right]$ with Galois group $S_4 / \left(\mathbb{Z}/2\mathbb{Z}\right)^2$. In other words, we have reduced the question to solving a cubic equation, since y_1, y_2, y_3 are just the roots of some third degree polynomial over $\mathbb{Q}$. We can work out this cubic with some messy algebra to get:

$$y^3 - 2by^2 + \left(b^2 - d\right)y + c^2 = 0 \tag{5.148}$$

so solving this cubic as above gives us the roots of our quartic polynomial.

Remark 5.33. Note as above, that to solve quartics, we reduced the question to cubics, and to solve cubics, we can reduce the question to solving quadratics. What about reducing a polynomial of degree 5 to degree 4? As it turns out, since S_5 is not solvable, if we follow the same procedure with a degree 5 polynomial, this yields a degree 6 polynomial, which is clearly even worse.

5.15 Galois cohomology

5.15.1 Definitions and examples

Example 5.64. Let G be a group acting on some module M. Then we look at two things:

1. The subset of things fixed by G, M^G. The invariants of G in M.
2. M_G: M modulo all the things of the form $m - gm$ for $m \in M$ and $g \in G$.

In particular, M^G is the largest submodule of M such that G acts trivially, and M_G is the largest quotient of M where G acts trivially.

Remark 5.34. This shows a general concept, that when you are concerned with invariants, you are likely also interested in the dual notion.

Proposition 5.28. *Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{5.149}$$

be an exact sequence. Then

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow 0 \tag{5.150}$$

only fails to be exact at the last morphism, and

$$0 \longrightarrow A_G \longrightarrow B_G \longrightarrow C_G \longrightarrow 0 \tag{5.151}$$

only fails to be exact at the first morphism.

Example 5.65. Consider the exact sequence:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \tag{5.152}$$

and let G act as -1 on the module $\mathbb{Z}$. Then as the previous proposition gives, the top sequence fails to be exact at the final morphism, since it is not onto, and the bottom sequence fails to be exact at the first morphism, since it is not injective.

$$\begin{gathered} 0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \end{gathered} \tag{5.153}$$

The key point here is that taking the invariants, or the funny dual notion does not preserve exactness.

We can rewrite invariant modules as follows:

$$M^G \cong \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \tag{5.154}$$

which is the set of homomorphisms preserving the action of G. Recall $\mathbb{Z}G$ is the group ring of G, so M is a module over $\mathbb{Z}G$, since if a group acts on something, so does its group ring. Note $\mathbb{Z}$ is a module over $\mathbb{Z}G$ with elements acting trivially. It is trivial to see this isomorphism. Just send the elements m fixed by G to the map from $\mathbb{Z}$ to M sending 1 to m. Recall that $\operatorname{Hom}(\cdot,\cdot)$ does not preserve exactness, however this failure is “controlled” by Ext.

Now note we can also rewrite the dual notion as:

$$M_G = \mathbb{Z} \otimes_{\mathbb{Z}G} M \tag{5.155}$$

and again, $\otimes$ does not preserve exactness, but the failure here is “controlled” by Tor. In detail, put

$$H^0(G, M) = M^G = \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \tag{5.156}$$

to be the zeroth cohomology group, and put the ith cohomology group to be

$$H^i(G, M) = \operatorname{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, M) \tag{5.157}$$

$H^i(G, M)$ is sometimes referred to as “H^i of G with coefficients in M.” Then the long exact sequence of Ext gives that if our sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{5.158}$$

is exact, so is:

$$0 \longrightarrow H^0(A) \longrightarrow H^0(B) \longrightarrow H^0(C) \longrightarrow H^1(A) \longrightarrow \cdots \tag{5.159}$$

In other words, this is just Ext with different notation. Similarly, we can put

$$H_0(G, M) = M_G \qquad\qquad H_i(G, M) = \operatorname{Tor}^{\mathbb{Z}G}_i(\mathbb{Z}, M) \tag{5.160}$$

so we get

$$\cdots \longrightarrow H_1(C) \longrightarrow H_0(A) \longrightarrow H_0(B) \longrightarrow H_0(C) \longrightarrow 0 \tag{5.161}$$

So we see that H^1 and H_1 effectively control the lack of exactness on M^G and M_G. The importance here is that these aren't typically so bad to calculate. Recall we worked out Tor of abelian groups and it wasn't so bad.

5.15.2 Alternative definition

Remark 5.35. In Lang's algebra [5], he introduces a notion of Galois cohomology which has effectively no explanation or motivation. How does our exposition relate to his?

Definition 5.20. A homomorphism $G \to M$ written $\sigma \mapsto a_\sigma$ is a *crossed homomorphism* iff we have that $a_{\sigma\tau} = a_\sigma + \sigma a_\tau$. In addition, this is a *principal crossed homomorphism* iff there is some b such that $a_\sigma = b/\sigma b$.

Remark 5.36. So this is the usual homomorphism with the extra σ term, so if G acts trivially this is just a homomorphism. This is somehow a notion of homomorphism which takes the action of G into account.

Proposition 5.29. *All principal crossed homomorphisms are crossed homomorphisms, but not the other way around.*

Definition 5.21. The first cohomology group is

$$H_1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}} \tag{5.162}$$

5.15.3 General form of Hilbert's theorem 90

Theorem 5.19. *For any Galois extension L/K, $H_0(G, L^\times) = 1$ where $G = \mathrm{Gal}(L/K)$.*

Proof. Suppose $a_\sigma \in L^\times$ and $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$. Now we want to find b such that $a_\sigma = b/\sigma b$ for all σ. So what is a crossed homomorphism here? Look at

$$\sigma \mapsto a_\sigma \cdot \sigma \tag{5.163}$$

this is a linear map from $L \to L$ and since $\tau \mapsto a_\tau \cdot \tau$ we have

$$\sigma\tau \mapsto a_{\sigma\tau} \cdot \sigma\tau = a_\sigma \cdot \sigma a_\tau \cdot \tau = (a_\sigma \cdot \sigma)(a_\tau \cdot \tau) \tag{5.164}$$

which is just the 1-cocycle condition. Then the homomorphism given by $\sigma \mapsto a_\sigma \sigma$ brings G to $\mathrm{End}(L)$. We can think of this as taking σ and twisting it by the cocycle.

Then we want to find b such that $a_\sigma \sigma b = b$ for all σ, where $b \neq 0$. In other words we just want b to be fixed by the twisting action. But we already know how to do this, we just take a generic fixed vector under G, only only fix it under the action $a_\sigma \sigma$. This gives our candidate:

$$b = \sum_{\sigma \in G} a_\sigma \cdot \sigma v \tag{5.165}$$

then as before, we just want to find v such that $b \neq 0$. Just cite lemma 5.4 to get that the elements σ are linearly independent, so we are finished. □

Remark 5.37. It is not obvious how this is equivalent to the other statement of Hilbert's theorem 90 in theorem 5.18.

Proposition 5.30. *If $N(a) = 1$ then we get a 1-cocycle given by $a_1 = 1, a_\sigma = 1$,*

$$a_{\sigma^2} = a \cdot \sigma a \cdots \tag{5.166}$$

and additionally we have some b where $a = b/\sigma b$ iff for all i, a cocycle is given by $a_{\sigma^i} = b/\sigma^i b$, meaning a 1-cocycle is a 1-coboundary. In other words, these two notions of Hilbert's theorem 90 are equivalent.

Proof. The statement from before took G to be cyclic, and $N(a) = 1$. Then we were to show that there is some b such that $a = b/\sigma b$. But how can we see that this is the same as a 1-cocycle? What is a 1-cocycle in this language? Let's put $a_1 = 1$, and $a_\sigma = 1$. Then

$$a_{\sigma^2} = a_\sigma \cdot \sigma a_\sigma = a \cdot \sigma a \tag{5.167}$$

$$a_{\sigma^3} = a_\sigma \cdot \sigma(a_{\sigma^2}) = a \cdot \sigma(a) \cdot \sigma^2(a) \tag{5.168}$$

meaning $N(a) = 1$ implies that we have the above 1-cocycle. □

Theorem 5.20 (Normal basis)**.** *L has a basis of the form $\{\sigma w : \sigma \in G\}$ for some fixed w.*

Proof. See Lang [5]. □

Theorem 5.21. *For any Galois extension L/K, if $G = \mathrm{Gal}(L/K)$ we have $H^1(G, L) = 0$*

Proof. The idea of this is to view it as a module over the group ring $K[G]$. Then $L \cong K[G]$ so it is a free module. But this just means L has a basis of some form $\{\sigma w : \sigma \in G\}$ for some fixed w. □

Corollary 5.3. *In fact, the normal basis theorem implies that*

$$H^i(G, L) = 0 \tag{5.169}$$

for all $i > 0$, since this vanishes for any free $K[G]$-module.

Example 5.66. So we have seen the first cohomology group of the multiplicative group $L^\times$ vanishes, and the cohomology groups of all orders vanish for L, so we might wonder if the cohomology groups vanish for all i for $L^\times$? It turns out this is not the case. To see this, note that

$$H^2\left(G, L^\times\right) \tag{5.170}$$

is non-zero. This is closely related to the Brauer group. Also, $H^1\left(G, L^\times\right)$ is closely related to the Picard group (which can both be defined for general schemes, not just fields.) Picard is only trivial over fields, however.

Theorem 5.22. *The definition given by Lang of the cohomology group is the same as ours. In other words,*

$$H^1 = Z^1/B^1 = \mathrm{Ext}^1_{\mathbb{Z}[G]}\left(\mathbb{Z}, M\right) \tag{5.171}$$

Sketch. To calculate $\mathrm{Ext}\left(A, B\right)$ we take the free resolution of A. In other words, we want the free resolution of $\mathbb{Z}$ by free $\mathbb{Z}\left[G\right]$ modules. Recall a resolution looks like this:

$$\begin{tikzcd}
\cdots \arrow[r, "d"] & \mathbb{Z}\left[G\right]\otimes\mathbb{Z}\left[G\right]\otimes\mathbb{Z}\left[G\right] \arrow[r, "d"] & \mathbb{Z}\left[G\right]\otimes\mathbb{Z}\left[G\right] \arrow[r, "d"] & \mathbb{Z}\left[G\right] \arrow[r, "d"] & \mathbb{Z} \arrow[r] & 0 \\
\cdots & g_0\otimes g_1\otimes g_2 & g_0\otimes g_1 & g_0 & 1 &
\end{tikzcd} \tag{5.172}$$

where the second row gives the $\mathbb{Z}$ bases. Note that G acts by

$$g\left(g_0\otimes g_1\otimes g_2\right) = gg_0\otimes gg_1\otimes gg_2 \tag{5.173}$$

Now we need to define the boundary such that $g_0\mapsto 1$, and

$$\begin{tikzcd}
g_0\otimes g_1 \arrow[r, mapsto] & g_1 - g_0 \\
g_0\otimes g_1\otimes g_2 \arrow[r, mapsto] & g_1\otimes g_2 - g_0\otimes g_1 + g_0\otimes g_1
\end{tikzcd} \tag{5.174}$$

now we can check that $d^2 = 0$, and if $da = 0$ then $a = d\cdot$something. Therefore we have an action of G which makes of these modules over $\mathbb{Z}\left[G\right]$.

Next we take the following free resolution:

$$F_1 \longrightarrow F_0 \longrightarrow A \longrightarrow 0 \tag{5.175}$$

look at

$$\begin{tikzcd}
\cdots & \mathrm{Hom}\left(F_2, B\right) \arrow[l] & \mathrm{Hom}\left(F_1, B\right) \arrow[l] \arrow[d, equal] & \mathrm{Hom}\left(F_0, B\right) \arrow[l] \arrow[d, equal] \\
 & & \left\{a_\sigma\in B : \sigma\in G\right\} & B
\end{tikzcd} \tag{5.176}$$

Here, $F_0 = \mathbb{Z}[G]$ so we can identify $\mathrm{Hom}(F_0, B)\, B$ where we sent $f \mapsto f(1)$. Then we can identify $\mathrm{Hom}(F_1, B) = \{a_\sigma\}$ since $a_\sigma = g(1 \otimes \sigma)$ and we can check that $d(a_\sigma) = 0$ iff $a_\sigma s$ for a 1-cocycle, and $\{a_\sigma\} = d(\bullet)$ iff a_σ are a 1-coboundary. □

Remark 5.38. If we are only interested in the first cohomology group, then it is fine to take Lang's definitions. If we are however interested in higher order cohomology groups, and wish to work abstractly, it is best to take our more abstract definition.

5.16 Infinite Galois extensions

5.16.1 Profinite groups and Krull topology

Definition 5.22. Let L/K be a field extension. This is a Galois extension iff it is normal, separable, and algebraic.

Remark 5.39. This is the full definition of a Galois extension. As it turns out, it is the same as our definition before, because before we assumed the extension to be finite, and hence algebraic. Now we are allowing for infinite extensions, which means we don't get this for free.

Example 5.67. The closure of $\mathbb{Q}$, $\overline{\mathbb{Q}}$ is an infinite Galois extension.

Example 5.68. Let L/K be an infinite Galois extension. $\mathrm{Gal}(L/K)$ hasn't changed in the infinite case in the sense that it is all of the automorphisms of L which leave K fixed. However, it isn't so clear what this group actually looks like. As it turns out, it is easy to describe this group in terms of the finite subextensions of L. Call the finite normal extensions $\{L_i\}_{i \in I}$. Then we have the following diagram:

$$\begin{tikzcd}
\cdots \arrow[dr, dash] & & L_3 \arrow[dl, dash] \arrow[dr, dash] & & \cdots \arrow[dl, dash] \\
& L_2 \arrow[dr, dash] & & L_1 \arrow[dl, dash] & \\
& & K & &
\end{tikzcd} \tag{5.177}$$

Now since any automorphism of L/K gives automorphisms of all the finite extensions L_i/K, we have the corresponding diagram of finite Galois groups. This shows us that an element of $\mathrm{Aut}(L/K)$ is a set of elements of the $\mathrm{Aut}(L_i/K)$ that are somehow compatible. Now we recognize this to be the inverse limit:

$$\varprojlim \mathrm{Gal}(L_i : K) \tag{5.178}$$

so the infinite case effectively reduces to the finite case.

Example 5.69. Take $K = \mathbb{F}_p$ and $L = \overline{\mathbb{F}}_p$ to be the algebraic closure. Then as we have seen, we can also describe L as the union of fields $\mathbb{F}_{p^k}$ for $k \geq 1$, though this is a strange sort of union. We have the diagram:

$$\begin{tikzcd}
\cdots & \cdots \arrow[dr, dash] & & \cdots \arrow[dr, dash] & \cdots \\
\mathbb{F}_{p^4} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^6} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^9} \\
& \mathbb{F}_{p^2} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{F}_{p^3} \arrow[ur, dash] & \\
& & \mathbb{F}_p \arrow[ur, dash] & &
\end{tikzcd} \tag{5.179}$$

Then again $\mathrm{Gal}\,(L/K)$ will be an inverse limit, since we have the diagram

$$\begin{tikzcd}
\cdots & \cdots \arrow[dr, dash] & & \cdots \arrow[dr, dash] & \cdots \\
\mathbb{Z}/4\mathbb{Z} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{Z}/6\mathbb{Z} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{Z}/9\mathbb{Z} \\
& \mathbb{Z}/2\mathbb{Z} \arrow[ur, dash] \arrow[dr, dash] & & \mathbb{Z}/3\mathbb{Z} \arrow[ur, dash] & \\
& & \mathbb{Z}/1\mathbb{Z} \arrow[ur, dash] & &
\end{tikzcd} \tag{5.180}$$

So we have

$$\mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right) = \varprojlim_n \left(\mathbb{Z}/n\mathbb{Z}\right) \tag{5.181}$$

which is called the profinite[5.16] completion of $\mathbb{Z}$.

Definition 5.23. Let G be a group, and G_i the normal subgroups of G such that G/G_i is finite. Then the profinite completion of G, is

$$\hat{G} = \varprojlim G/G_i \tag{5.182}$$

Recall the subgroups G_i form an inverse system, since they are partially ordered by inclusion.

Remark 5.40. We want to discuss continuity and density in $\hat{G}$, which motivates the following definition.

Definition 5.24. Let G be a group, and let G_i run over the normal subgroups of finite index. Then equip each G/G_i with the discrete topology, and given $\prod G/G_i$ the induced product topology. Then we give the restriction of $\prod G/G_i$ to $\varprojlim G/G_i$ the subset topology. This is known as the *Krull topology.*

Proposition 5.31. *The map $\eta : G \to \hat{G}$ is a homomorphism, and* $\mathrm{im}\,(\eta)$ *is dense in $\hat{G}$ equipped with the Krull topology. The map η also has the universal*

[5.16] This name comes from the fact that the inverse limit is also referred to as a projective limit. So this is somehow a projective finite completion.

property: given any profinite group H and group homomorphism $f : G \to H$, there exists a unique continuous group homomorphism from $g : \hat{G} \to H$ such that $f = g \circ \eta$.

Example 5.70. This gives the interpretation of $\varprojlim \mathbb{Z}/n\mathbb{Z}$ as some sort of topological completion of $\mathbb{Z}$. Explicitly, we have that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_i^{k_i}\mathbb{Z} \tag{5.183}$$

where $n = \prod_i p_i^{k_i}$. Then by the Chinese remainder theorem, we have

$$\varprojlim \mathbb{Z}/n\mathbb{Z} = \prod \varprojlim_{k_i} \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z}\right) = \prod_p \mathbb{Z}_p \tag{5.184}$$

where $\mathbb{Z}_p$ denotes the p-adic integers. See example 2.29 for more.

5.16.2 Galois correspondence

Example 5.71. We now investigate the extension of Galois correspondence to infinite Galois extensions. Let L/K be a Galois extension. Then take any $\alpha \in L$. Clearly $K[\alpha]/K$ is a finite extension. Now consider $\mathrm{Gal}(K[\alpha]/K)$. The subset of this group consisting of elements fixing α, is a closed subset of the Krull topology. We can see this, because it's just the things fixing α in M/K, where M is the normal closure of α. So the subgroup fixing any $\alpha \in L$ is always closed in the Krull topology. This means the subgroup fixing all elements of M, is the intersection of closed subgroups, and is therefore also closed. This motivates the notion that only closed subgroups should correspond to extensions. We see this formally in the following theorem.

Theorem 5.23. *Let L/K be a Galois extension of arbitrary degree. Then the subextensions are in correspondence with the closed subgroups of* $\mathrm{Gal}(L/K)$.

Proof. This is effectively the same as the finite case only with some routine book-keeping added. □

Example 5.72. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}_{\text{cycl}}$ to be the cyclotomic extension of $\mathbb{Q}$. That is $\mathbb{Q}$ with all roots of unity adjoined. We are adding these because extensions without "enough" roots of unity are obnoxiously difficult. Setting ζ_n to be the primitive n-th roots of unity, we can write:

$$L = \bigcup_n \mathbb{Q}[\zeta_n] \tag{5.185}$$

then we have the following diagram:

$$\begin{tikzcd}
\cdots & & \cdots \arrow[dl, dash] \arrow[dr, dash] & & \cdots \arrow[dl, dash] \arrow[dr, dash] & & \cdots \\
& \mathbb{Q}[\zeta_9] \arrow[dr, dash] & & \mathbb{Q}[\zeta_6] \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Q}[\zeta_4] \arrow[dl, dash] & \\
\cdots \arrow[drrr, dash] & & \mathbb{Q}[\zeta_3] \arrow[dr, dash] & & \mathbb{Q}[\zeta_2] \arrow[dl, dash] & & \cdots \arrow[dlll, dash] \\
& & & \mathbb{Q} & & &
\end{tikzcd} \tag{5.186}$$

note that $\mathbb{Q}[\zeta_2] = \mathbb{Q}$. We know that

$$\operatorname{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times \tag{5.187}$$

which consists of all maps from $\zeta_n \to \zeta_n^i$ for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. So the Galois group of $\mathbb{Q}_{\text{cycl}}/\mathbb{Q}$ is the inverse limit of the diagram

$$\begin{tikzcd}
\cdots & \cdots \arrow[dl, dash] \arrow[dr, dash] & & \cdots \arrow[dl, dash] \arrow[dr, dash] & \cdots \\
(\mathbb{Z}/9\mathbb{Z})^\times \arrow[dr, dash] & & (\mathbb{Z}/6\mathbb{Z})^\times \arrow[dl, dash] \arrow[dr, dash] & & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[dl, dash] \\
\cdots \arrow[drr, dash] & (\mathbb{Z}/3\mathbb{Z})^\times \arrow[dr, dash] & & (\mathbb{Z}/2\mathbb{Z})^\times \arrow[dl, dash] & \cdots \arrow[dll, dash] \\
& & (\mathbb{Z}/1\mathbb{Z})^\times & &
\end{tikzcd} \tag{5.188}$$

Recall this is different from the finite field case, because we are now dealing with the multiplicative groups, rather than the additive ones. We can write:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \prod \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z}\right)^\times \tag{5.189}$$

so we can write:

$$\varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \prod_p \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z}\right)^\times = \prod_p \mathbb{Z}_p^\times = \overline{\mathbb{Z}}^\times \tag{5.190}$$

where $\bar{\mathbb{Z}}$ is the profinite completion of the ring $\mathbb{Z}$. At least it is abelian...

Example 5.73. Take $L = \overline{\mathbb{Q}}$ and $K = \mathbb{Q}$. We might wonder what $G = \operatorname{Gal}(L/K)$ is. This turns out to be a very difficult question. We know

$$G^{\mathbf{Ab}} = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \tag{5.191}$$

We also have the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}_{\text{cycl}}\right) \arrow[r] & \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \arrow[r] & \operatorname{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q}) \arrow[r] \arrow[d, equal] & 0 \\
& & & \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times &
\end{tikzcd} \tag{5.192}$$

where $\varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$ is the maximal abelian quotient.

Conjecture 1 (Shafarevich)**.** *The Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}_{cycl}$ is isomorphic to the profinite completion of a countable free group.*

Remark 5.41. The Langlands program concerns $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and is related to automorphic forms. Some of Wiles' proof of Fermat's last theorem in fact have to do with understanding the structure of $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$.

5.17 Kummer theory

The general idea of Kummer theory is to find arbitrary extensions of a field K given K has "enough" roots of unity. If there are "not enough" roots of unity, this is more like class field theory. We will be combining some elements of Galois cohomology and infinite Galois extensions.

Example 5.74. Let's consider a high-powered version of this. Let $\overline{K}$ be the separable algebraic closure of K. This is the largest separable extension in the algebraic closure. Assume $(n, p) = 1$ where $p = \operatorname{char}(K)$. Now look at the following exact sequence of groups acted on my $\operatorname{Gal}\left(\overline{K}/K\right)$:

$$\begin{tikzcd}
1 \arrow[r] & \mu_n \arrow[r] & \overline{K}^\times \arrow[r] & \overline{K}^\times \arrow[r] & 1 \\
 & & x \arrow[r, mapsto] & x^n &
\end{tikzcd} \tag{5.193}$$

where μ_n denotes the nth roots of unity, and we have assumed $\mu_n \subseteq K$, in the sense that we have "enough" roots of unity. Now take the invariants under the Galois group of this sequence. Recall this does not preserve exactness. In other words, we have to use some Galois cohomology to get a proper exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & \mu_n \arrow[r] & K^\times \arrow[r, "x\mapsto x^n"] & K^\times \arrow[dlll, hook] \\
H^1\left(G, \mu_n\right) \arrow[r] \arrow[d, equal] & H^1\left(G, \overline{K}^\times\right) \arrow[r] \arrow[d, equal] & H^1\left(G, \overline{K}\right) \arrow[r] \arrow[d, equal] & \cdots \\
\operatorname{Hom}\left(G, \mu_n\right) & 1 & 1 &
\end{tikzcd} \tag{5.194}$$

where the bottom line for $H^1\left(G, \mu_n\right)$ follows from the fact that G acts trivially on μ_n, and the rest of this line follows from Hilbert's theorem 90 (theorems 5.18 and 5.19. Now from this sequence, we can read off a cyclic extension of degree n of K. We have our simplified sequence

$$K^\times \longrightarrow K^\times \longrightarrow \operatorname{Hom}\left(G, \mu_n\right) \longrightarrow 1 \tag{5.195}$$

where $\operatorname{Hom}\left(G, \mu_n\right)$ is cyclic of order n, and we still have $x \mapsto x^n$ in the map from $K^\times$ to itself. So we have that

$$\operatorname{Hom}\left(G, \mu_n\right) = K^\times / \left(K^\times\right)^2 \tag{5.196}$$

consists of the elements of $K^\times$ modulo nth powers. Then we have that the kernels of these maps are subgroups $H \subseteq G$ with G/H cyclic, and order dividing n. Then this is isomorphic to the extensions L/K with $\operatorname{Gal}\left(L/K\right)$ cyclic with order dividing n. In short, we obtained a description of these using Galois cohomology. Note this is effectively the same process as the earlier description, where we found that cyclic extensions have the form $K\left[\sqrt[n]{\bullet}\right]$. The advantage here, is just that we are working more generally. Recall, however, that we assumed this was a cyclic extension of order coprime to the characteristic. We generalize this in the next example.

Example 5.75. Recall in the case of finite Galois extensions we started with the case analogous to the previous example with a cyclic extension with order coprime to the characteristic. We then generalized and ended up with the concept of an Artin-Schreier equation. We now make the analogous generalization. Let L/K be a cyclic extension of order p, where $p = \operatorname{char}(K)$. Then we can take $L = K[\alpha]$ where α is a root of $x^p - x - b$ for $b \in K$. Now we want to rewrite this in terms of infinite extensions and Galois cohomology. As before, we have an exact sequence:

$$\begin{gathered} 0 \longrightarrow \mathbb{F}_p \longrightarrow \overline{K} \xrightarrow{\ f\ } \overline{K} \longrightarrow 0 \\ x \longmapsto x^p - x \end{gathered} \tag{5.197}$$

where we are working with the additive groups $\overline{K}$ again. Then $\ker(f) = \mathbb{F}_p$ since these are just the roots of $x^p - x$. So this is again just an exact sequence of modules acted on by $\operatorname{Gal}\left(\overline{K}/K\right)$. Now take the invariants of this sequence to get:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}_p \arrow[r] & K \arrow[r] & K \arrow[r] & H^1(G,\mathbb{F}_p) \arrow[r] \arrow[d, equal] & H^1\left(G,\overline{K}\right) \arrow[r] \arrow[d, equal] & H^1(G,K) \arrow[r] \arrow[d, equal] & \cdots \arrow[d, equal] \\ & & & & \operatorname{Hom}(G,\mathbb{F}_p) & 0 & 0 & 0 \end{tikzcd} \tag{5.198}$$

where the first element of the second line is because G acts trivially on $\mathbb{F}_p$ and the rest are a result of the normal basis theorem. Now we can write

$$\operatorname{Hom}(G,\mathbb{F}_p) = K/\operatorname{im}(x^p - x) \tag{5.199}$$

which gives an explicit group defined in terms of the field. Therefore these correspond to the minimal subgroups of index p which correspond to cyclic extensions of degree p.

Example 5.76. There is a minor gap in the above treatment. We might want an extension L/K with:

$$\operatorname{Gal}(L/K) = \mathbb{Z}/p^n\mathbb{Z} \tag{5.200}$$

for $n > 1$. To get such an extension, we can use something called Witt vectors. For more on this see the exercises in Lang [5]. In short, we get an exact sequence:

$$0 \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow W \longrightarrow W \longrightarrow 0 \tag{5.201}$$

where W is the ring of Witt vectors. Then we can describe all cyclic extensions of fields as long as they contain sufficient roots of unity.

Bibliography

[1] L.V. Ahlfors, *Complex analysis*, 1966.

[2] J.W. Brown and R.V. Churchill, *Complex variables and applications*, Brown-Churchill series, McGraw-Hill Higher Education, 2004.

[3] R. Hartshorne, *Algebraic geometry*, Encyclopaedia of mathematical sciences, Springer, 1977.

[4] S. Lang, *Algebraic number theory*, Applied Mathematical Sciences, Springer, 1994.

[5] ______, *Algebra*, Graduate Texts in Mathematics, Springer New York, 2005.