

Algebra I Bootcamp Notes

Ryan Wandsnider

August 4, 2026

Abstract

These are notes for the Algebra I Bootcamp held in Summer 2026.

1 Basic Group Theory

Definition 1.1. A *group* is a set G with a binary operation $\cdot$ satisfying

- i. associativity
- ii. existence of an identity
- iii. existence of inverses

If $\cdot$ is commutative G is an *abelian* group.

Examples 1.2. i. $\mathbb{Z}$ under addition.

- ii. $\mathbb{Z}_n$, the integers modulo n , under addition mod n .
- iii. The free group on n letters F_n is the set of all finite words of $x_1, \dots, x_n$ with multiplication given by concatenation. It is “maximally non-abelian” in some sense.

Definition 1.3. A subgroup of G is a subset $H \subset G$ containing e which is closed under $\cdot$ and $(\bullet)^{-1}$. We denote subgroup by $\leq$.

Example 1.4. Every G has the trivial subgroup and the subgroup which is G itself.

Example 1.5. The *center* of a group is the subgroup

$$Z(G) := \{g \in G \mid gh = hg, \forall h \in G\} \leq G.$$

It is possible that an element of g commutes (or centralizes) a few elements, but not all of them. We define the *centralizer* of a subset $X \subset G$ to be the subgroup

$$Z_G(X) = \{g \in G \mid gx = xg, \forall x \in X\}.$$

Then, $Z(G) = Z_G(G)$.

Definition 1.6. Given a subset $X \subset G$, the subgroup generated by X is the smallest subgroup of G containing X and is denoted

$$\langle x \mid x \in X \rangle \leq G.$$

Example 1.7. For any $g \in G$, $\langle g \rangle$ is a subgroup of G . A group G is *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle$.

Definition 1.8. Given a subgroup $H \leq G$, the *left cosets* are

$$gH = \{gh \mid h \in H\}$$

and the right cosets are

$$Hg = \{hg \mid h \in H\}.$$

Denote the set of cosets by

$$G/H = \{gH \mid g \in G\}$$

If G/H is a finite set, define $[G : H] := |G/H|$ to be the *index* of H in G .

Proposition 1.9. If $H \leq G$, then $|H| \cdot [G : H] = |G|$. For $g \in G$, $\langle g \rangle$ is a cyclic subgroup of G of order equal to the order of g ; hence $\text{ord}(g)$ divides $|G|$.

Definition 1.10. A *group homomorphism* between groups G, H is a map $\phi: G \rightarrow H$ such that $\phi(e) = e$ and $\phi(gg') = \phi(g)\phi(g')$. If ϕ is bijective, then ϕ^{-1} is also a homomorphism and we call ϕ an isomorphism. An automorphism is an isomorphism of a group with itself.

Example 1.11. For any $g \in G$, the map $c_g: G \rightarrow G$ defined by $c_g(x) = gxg^{-1}$ is a group homomorphism, called *conjugation by g* .

Example 1.12. For any group G , the set of automorphisms $\text{Aut}(G)$ is a group under composition.

Definition 1.13. A subgroup $N \leq G$ is *normal* if $gNg^{-1} \subset N$ for all $g \in G$, where

$$gNg^{-1} := c_g(N) = \{gng^{-1} \mid n \in N, g \in G\}.$$

Equivalently, we have $gNg^{-1} = N$ for all $g \in G$. We denote normal subgroup by $N \trianglelefteq G$.

It is possible for only some $g \in G$ to satisfy $gNg^{-1} = N$. We define the *normalizer* of N to be

$$N_G(N) := \{g \in G \mid gNg^{-1} = N\}.$$

Then, N is normal if and only if $N_G(N) = G$.

Definition 1.14. The *kernel* and *image* of a group homomorphism $\phi: G \rightarrow H$ are

$$\ker \phi := \{g \in G \mid \phi(g) = e\}$$

and

$$\text{im } \phi := \{\phi(g) \mid g \in G\} \subset H.$$

$\ker \phi$ is always a normal subgroup of the domain and $\text{im } \phi$ is always a subgroup of the codomain that need not be normal.

Definition 1.15. Given a normal subgroup $N \trianglelefteq G$, we can define a group structure on G/N called the quotient group, with $\cdot$ defined by

$$gH \cdot g'H = gg'H.$$

It comes with a natural surjective homomorphism $q: G \rightarrow G/N$ defined by $q(g) = gN$ with kernel N .

Remark 1.16. A key fact used in the well-definedness of quotient groups is that $gH = Hg$ for all g if and only if H is normal; this is obvious from the definition of normal subgroup.

Remark 1.17. The quotient group is the unique group structure on G/N such that q is a homomorphism, and such a structure exists if and only if N is normal.

Hence, a subgroup $K \leq G$ is normal if and only if there is some group H and group homomorphism $\phi: G \rightarrow H$ such that $K = \ker \phi$.

Remark 1.18. In an abelian group G , every subgroup is normal.

Remark 1.19. By specifying generators and relations we can define a group as a quotient of a free group by a normal subgroup. For example,

$$\langle a, b \mid aba^{-1} = b \rangle := F_2/N$$

where N is the smallest normal subgroup of F_2 containing $aba^{-1}b^{-1}$. This group is of course just the product $\mathbb{Z} \times \mathbb{Z}$ with componentwise product.

Example 1.20. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example 1.21. The *quaternion group* Q_8 is the group

$$\langle -1, i, j, k \mid (-1)^2 = i^2 = j^2 = k^2 = 1, ijk = -1 \rangle.$$

Definition 1.22. Given H, K groups, the product group is $H \times K$ with $(h, k) \cdot (h', k') := (hh', kk')$.

Fact 1.23. $H \times K$ is abelian if and only if H and K are both abelian.

Definition 1.24. If $\{H_n\}_{n \in \mathbb{N}}$ is an infinite collection of groups, there are two natural ways to define their product. The *direct product* of the collection is

$$\prod_{n \in \mathbb{N}} H_n = \{(h_n)_{n \in \mathbb{N}} \mid h_n \in H_n\}$$

and the *direct sum* of the collection is

$$\bigoplus_{n \in \mathbb{N}} H_n = \{(h_n)_{n \in \mathbb{N}} \mid h_n \in H_n, h_n = 0 \text{ for all but finitely many } n\}.$$

If the H_n are all abelian, the direct product is the categorical product and the direct sum is the categorical coproduct.

A generalization of the product is the *semi-direct product*, which arises when G is a product of subgroups H and N as a set, but these subgroups don't quite commute with each other.

Definition 1.25. We first discuss the *outer* semi-direct product. Suppose H and N are groups, and $\varphi: H \rightarrow \text{Aut}(N)$ is a group homomorphism. We define the *semi-direct product* $N \rtimes_{\varphi} H$ to be the set $N \times H$ with multiplication

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh')$$

Observe that $N \leq N \rtimes_{\varphi} H$ and $H \leq N \rtimes_{\varphi} H$ via the natural embeddings $n \mapsto (n, 1)$ and $h \mapsto (1, h)$. Furthermore,

$$c_h(n) = (1, h)(n, 1)(1, h^{-1}) = (\phi_h(n), h)(1, h^{-1}) = (\phi_h(n), 1) \in N.$$

Hence, $N \trianglelefteq N \rtimes_{\varphi} H$, and conjugation by h coincides with ϕ_h .

Definition 1.26. The *inner* semi-direct product realizes a group as a semi-direct product of its subgroups. Suppose G is a group with subgroups N and H such that $N \cap H = 0$, $N \trianglelefteq G$, and $NH = G$, i.e. every element of G can be written uniquely as a product hn for $h \in H$ and $n \in N$.

Define $\varphi: H \rightarrow \text{Aut}(N)$ by $\varphi(h) = c_h$. Then, the map

$$N \rtimes_{\varphi} H \rightarrow G$$

given by $(n, h) \mapsto nh$ is an isomorphism.

Example 1.27. For every $n \in \mathbb{N}$, the *dihedral group* of order $2n$ is the set D_n of symmetries of a n -gon. It is generated by a rotation r and a reflection s :

$$D_n := \langle r, s \mid r^n = s^2 = e, rs = sr^{n-1} \rangle$$

It is not hard to see that $\langle s \rangle$ normalizes $\langle r \rangle$, and conjugation by s acts by the automorphism $r \mapsto r^{n-1}$. Hence,

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$

for $\varphi(1) = (a \mapsto (n-1) \cdot a)$.

Example 1.28. Q_8 is *not* a semi-direct product.

Exercise 1.29. Classify groups of order pq for p and q prime.

Remark 1.30. Given groups N, H , an *extension*¹ of H by N is a group G fitting into a short exact sequence

$$1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1,$$

meaning the kernel of every map out coincides with the image of every map in, i.e. α is injective, β is surjective, and $\ker \beta = \text{im } \alpha$. It is called a *central extension* if $N \leq Z(G)$.

Observe

¹The terminology feels a bit backwards to me, because N is the one appearing as a subgroup and H appears as a quotient.

- i. G is a semi-direct product if, and only if, this sequence *splits*, meaning there is a map $\gamma: H \rightarrow G$ such that $\beta \circ \gamma = \text{id}_H$ (i.e. a *section* of β).²
- ii. G is a direct product if, and only if, this sequence splits via a map $\gamma: H \rightarrow G$ and $\gamma(H)$ commutes with N .
- iii. If the sequence splits and the extension is central, then G is necessarily a direct product.

Definition 1.31. For any groups G, H with H abelian, the set $\text{Hom}(G, H)$ of homomorphisms $G \rightarrow H$ forms a group under pointwise multiplication.

Problem (Aug 2024, 1). a. Let G be a group and A an abelian group. Define a group structure on $\text{Hom}(G, A)$. Is it abelian?

- b. Prove or disprove: $\text{Hom}(\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ and $\text{Hom}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$ are isomorphic as groups.

Remark 1.32. Homomorphisms out of a direct product is equivalent to a pair of homomorphisms out of each of the components.

Lemma 1.33 (Unnamed Lemma). Suppose $\phi: G \rightarrow H$ is a homomorphism and let $K = \ker \phi$. Then, there exists $\tilde{\phi}: G/K \rightarrow H$ such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ q \downarrow & \nearrow \tilde{\phi} & \\ G/K & & \end{array}$$

commutes. It is defined by $\tilde{\phi}(gK) = \phi(g)$.

Theorem 1.34 (Isomorphism Theorems).

- I. If $\phi: G \rightarrow H$ is a surjective homomorphism and $K = \ker \phi$, the induced map $\tilde{\phi}: G/K \rightarrow H$ is an isomorphism.
- II. Let $H \leq G$ and $N \trianglelefteq G$. Then, $N \cap H$ and NH are subgroups of G . Furthermore, $N \cap H \trianglelefteq H$ and $N \trianglelefteq NH$, and the map $H/(N \cap H) \rightarrow NH/N$ defined by $h(N \cap H) \mapsto hN$ is a well-defined isomorphism

$$H/(N \cap H) \cong NH/N.$$

- III. (Lattice Isomorphism Theorem) If N, K are normal subgroups of G and $N \leq K$, the map $G/K \rightarrow (G/N)/(K/N)$ defined by $gK \mapsto g(K/N)$ is a well-defined isomorphism

$$G/K \cong (G/N)/(K/N).$$

²For example, let $G = S^1 \times S^1 / \pm(1, 1)$, $N = (\pm 1, \pm 1) / \pm(1, 1)$, and $H = S^1 \times S^1 / (\pm 1, \pm 1)$. However, this sequence cannot split (for topological reasons).

IV. (Correspondence Theorem) Suppose $N \trianglelefteq G$. Then, there is a bijective correspondence

$$\{\text{subgroups of } G \text{ containing } N\} \leftrightarrow \{\text{subgroups of } G/N\}$$

given by $\tilde{K} \mapsto \tilde{K}/N$. Furthermore, $\tilde{K}$ is normal in G if, and only if, $\tilde{K}/N$ is normal in G/N .

2 Solvability and Simplicity

Definition 2.1. A group is *simple* if it has no proper nontrivial normal subgroups.

Example 2.2. For p prime, $\mathbb{Z}/p\mathbb{Z}$ is simple.

Definition 2.3. A group G is *solvable* if there exists a finite sequence of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

such that $G_i \trianglelefteq G_{i+1}$ (but not necessarily normal in G) and the successive quotients G_{i+1}/G_i are abelian.

Example 2.4. Any p -group is solvable; every p -group has nontrivial center – see group action section.

Problem (Jan 2021, 1). A group is called elementary abelian p -group if it is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some n . Suppose G is a solvable finite group. Prove it has an elementary abelian subgroup A which is *characteristic* in G , i.e. $\sigma(A) = A$ for all $\sigma \in \text{Aut}(G)$.

Hint: Use $x \mapsto x^p$.

Theorem 2.5 (Burnside's Theorem). Every group of order $p^a q^b$ is solvable.

Problem (Jan 2025, 1). Prove or disprove: there is a simple group of order 2025.

3 Symmetric Groups

We now discuss a few facts about the group S_n .

Definition 3.1. The *symmetric group* on n elements is the set S_n of bijections σ of the set $\{1, \dots, n\}$ with itself. It is a group under composition.

Definition 3.2. A k -cycle in S_n is a permutation σ which fixes all but a set of k elements, which it cycles. For $i_1, \dots, i_k \in \{1, \dots, n\}$, $\sigma(i_j) = \sigma(i_{j+1})$ for $1 \leq j \leq k-1$, and $\sigma(i_k) = i_1$. It is denoted

$$\sigma = (i_1 \ i_2 \ \dots \ i_k).$$

Fact 3.3. Every permutation is a product of disjoint cycles (cycles of disjoint subsets of $\{1, \dots, n\}$).

In fact, conjugacy classes of permutations are classified by cycle type: two permutations are conjugate by an element of S_n if and only if they have cycle decompositions with the same cycle lengths appearing.

Fact 3.4. Every permutation is a product of 2-cycles. Furthermore, the parity (even/odd) of the number of 2-cycles appearing in any decomposition is the same. This number modulo two is called the *sign* of the permutation. This defines a group homomorphism

$$\text{sgn}: S_n \rightarrow \{\pm 1\}.$$

Its kernel is the *alternating group*, denoted A_n .

Fact 3.5. $A_n \trianglelefteq S_n$, and it is the only proper nontrivial normal subgroup of S_n .

Fact 3.6. A_n is simple for $n \geq 5$. (Important)

Fact 3.7. $|S_n| = n!$ and $|A_n| = n!/2$.

Trick 3.8. It is extremely common in problems to obtain a homomorphism $S_n \rightarrow G$. Because kernels are normal, there are only three possibilities for the kernel of this map.

4 Group Actions

Remark 4.1. At least one prelim question always seems to require group actions and the orbit-stabilizer theorem.

Definition 4.2. A *group action* of a group G on a set X is either of the following equivalent definitions

- i. a group homomorphism $G \rightarrow \text{Perm}(X)$
- ii. a map $G \times X \rightarrow X$ denoted $(g, x) \mapsto g \cdot x$ such that $e \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$.

Definition 4.3. Suppose G acts on a set X . The *orbit* of $x \in X$ is the set

$$G \cdot x := \{g \cdot x \mid g \in G\} \subset X.$$

The *stabilizer* of $x \in X$ in G is the subgroup

$$\text{Stab}_G(x) := \{g \in G \mid g \cdot x = x\} \leq G.$$

Definition 4.4. A *fixed point* of an action is $x \in X$ such that $g \cdot x = x$ for all $g \in G$. Equivalently, if $G \cdot x = \{x\}$ or $\text{Stab}_G(x) = G$.

Definition 4.5. We say an action is *transitive* if the orbit of any $x \in X$ is all of X . We say the action is *n-transitive* if for any two n -tuples $(x_1, \dots, x_n)$ and $(x'_1, \dots, x'_n)$ of elements of X , there exists a single g such that $g \cdot x_i = x'_i$ for all i .

Example 4.6. For $H \leq G$ a subgroup, there are two extremely common and useful actions of G .

- a. G acts on the cosets G/H by left multiplication. This action is always transitive, and the stabilizer of a coset gH is the group gHg^{-1} .
- b. Let X denote the set of all subgroups of G conjugate to H . Then, G acts transitively on X by conjugation. This action is particularly useful for Sylow subgroups.

Trick 4.7. A group action of G on a set of n elements is the same data as a group homomorphism $G \hookrightarrow S_n$. This can be used to derive a contradiction in a proof if $|G|$ does not divide $n!$.

Theorem 4.8 (Orbit-Stabilizer). Suppose a finite group G acts on a set X . Then, for any $x \in X$,

$$|G| = |G \cdot x| \cdot |\text{Stab}_G(x)|.$$

Corollary 4.9. If G is a p -group (meaning its order is a power of p) acting on a finite set of size n with m fixed points, then $m \equiv 1 \pmod{p}$.

Exercise 4.10. Prove this using the theorem.

Exercise 4.11. Prove that the center of any p -group is non-trivial.

Problem (Aug 2020, 1). Let G be a group of order p^k for some prime p and $k \geq 1$. Show that for every $1 \leq l \leq k$ that G has a normal subgroup of order p^l . Prove this from first principles.

Problem (Jan 2024, 1). a. Let G be a finite group. Assume the intersection of all non-trivial subgroups of G is non-trivial. Suppose G acts faithfully on the finite set X (i.e. the map $G \rightarrow \text{Perm}(X)$ is injective). Show $|X| \geq |G|$.

- b. Let Q be the quaternion group (of order 8). Find the smallest n such that Q is isomorphic to a subgroup of the symmetric group S_n .

Problem (Aug 2023, 2a). Prove that a finite group is not the union of conjugates of any proper subgroup.

Problem (Jan 2023, 1). a. Let G be a finite group of order n . Let m be an integer coprime to n . Suppose g and h are elements of G with $g^m = h^m$. Show that $g = h$.

- b. Suppose that G is a finite simple group. Let p be the largest prime dividing $|G|$. Show that G has no proper subgroup with $[G : H] < p$.

Problem (Aug 2020, 2). Let n be an odd number so that $\pi = (1 \ 2 \ \dots \ n) \in A_n$. Is the S_n -conjugacy class of π the same as its A_n -conjugacy class?

5 Sylow Theorems

Let G be a finite group of order n .

Theorem 5.1. For every prime $p \mid n$, there exists a p -Sylow subgroup of G , i.e. a subgroup of order p^k for the maximal k such that $p^k \mid n$.

Theorem 5.2. Every p -Sylow subgroup of G is conjugate.

Theorem 5.3. Denote by n_p the number of Sylow subgroups of G , and write $n = p^k m$ for p^k the order of a p -Sylow subgroup. Then,

- i. $n_p \mid m$
- ii. $n_p \equiv 1 \pmod{p}$
- iii. $n_p = [G : N_G(P)]$, the index in G of the normalizer of P .

Remark 5.4. Note that $n_p = 1$ if and only if any p -Sylow subgroup (and necessarily the only one) is normal.

Trick 5.5. A common problem is computing n_p . The technique is typically:

- a. Rule out possibilities by the restrictions $n_p \in \{1, p+1, 2p+1, \dots\}$ and $n_p \mid m$.
- b. Use order considerations to rule out the bigger ones.

Exercise 5.6. Show that, for $p < q$ primes, any group of order pq has a normal subgroup of order q .

Trick 5.7. It is extremely common to use that all p -Sylow subgroups are conjugate to compute n_p . The natural action of G on the collection of p -Sylow subgroups is always transitive.

Problem (Jan 2021, 2). Show that if $|G| = 132 = 2^2 \cdot 3 \cdot 11$, then G is not simple.

Problem (Aug 2023, 3). Let p be the smallest prime dividing the order of a finite group G , and $H \subset G$ a subgroup of index p . Show that H is normal.

Problem (Jan 2022, 1).
a. Let p a prime. Prove that every group of order p^2 is abelian.
b. Determine the number of isomorphism classes of groups of order 45.

Problem (Aug 2021, 1). Let H be a simple group of order 60. Prove that $H \cong A_5$ and determine all p -Sylow subgroups of H up to isomorphism.

Problem (Aug 2025, 1). Let G be a group of order $504 = 2^3 3^2 7$.

- a. Prove that G is not isomorphic to a subgroup of the alternating group A_7 .

- b. Assume G is simple, then determine the number of 3-Sylow subgroups of G .

Problem (Jan 2024, 2). Let F be the set of Sylow 5-subgroups of S_5 .

- Prove that the elements of F are exactly the subgroups generated by 5-cycles, and $|F| = 6$. Explain why this gives an injective homomorphism $\varphi: S_5 \hookrightarrow S_6 = \text{Perm}(F)$, with image a transitive subgroup. Set $H := \text{im}(\varphi) \subset S_6$. Prove $|S_6/H| = 6$.
- Prove that H is not conjugate to any of the obvious $S_5 \subset S_6$ (stabilizers of elements of F).
- Prove that S_6 has an outer automorphism, i.e. an automorphism not given by conjugation.

You may use without proof the standard fact that $A_n \subset S_n$ is the only non-trivial proper normal subgroup for any $n \neq 4$.

Problem (Aug 2022, 2). a. Let G be a finite group and let $H \trianglelefteq G$ be a normal subgroup. Let $P \subset H$ be a p -Sylow subgroup of H . Let $N_G(P)$ (resp. $N_H(P)$) be the normalizer of P in G (resp. H). Show that the natural map

$$H/N_H(P) \rightarrow G/N_G(P)$$

is a bijection. Deduce that $H \cdot N_G(P) = G$.

- b. Let K be a finite group and let $P \subset K$ be a p -Sylow subgroup. Show that

$$N_K(N_K(P)) = N_K(P).$$

Hint: use (a).

Problem (Aug 2022, 3). Let G be a group of order $833 = 7^2 \cdot 17$. Let S be a set of order 32 on which G acts.

- Show that there necessarily exists a fixed point for the action, i.e. there exists $x \in S$ with $g \cdot x = x$ for all $g \in G$.
- For given G of order 833 show there necessarily exists a set S with a G -action such that $|S| = 32$ and there exists exactly one fixed point.

Problem (Jan 2020, 2). Throughout this problem G will always be a group of order 27, but not necessarily the same group in each part.

- Show that if G has a subgroup H of order three which is not normal, G is isomorphic to a subgroup of S_9 .
- Suppose $x \in S_9$ is an element of order 9. Find the orders of $C_{S_9}(\langle x \rangle)$ and $N_{S_9}(\langle x \rangle)$.
- Suppose $x \in S_9$ is an element of order 9. Describe the 3-Sylow subgroup of $N_{S_9}(\langle x \rangle)$.
- Up to isomorphism, there are four group of order 27 which contain an element of order 9. List any that can be embedded in S_9 and justify why your list is correct.

6 Basic Ring Theory

Definition 6.1. A *ring* is a set R with two binary operations $+, \cdot$ such that $(R, +)$ is an abelian group with identity 0, $\cdot$ is associative with identity 1, and $\cdot$ distributes over $+$ on the left and right.

If $\cdot$ is commutative we say R is a *commutative ring*. It only pays to study commutative rings for the prelims. We will always assume rings are commutative unless specifically stated.

Examples 6.2. i. $(\mathbb{Z}, +, \times)$

ii. $(\mathbb{R}, +, \times)$

iii. $(\mathbb{C}, +, \times)$

iv. $\mathbb{Z}_n$, the integers modulo n , with addition and multiplication modulo n

v. $R[x]$, the ring of formal polynomials with coefficients in another ring R

vi. $R[x_1, \dots, x_n]$.

Example 6.3. The set of $n \times n$ matrices with coefficients in any ring R under matrix addition and multiplication is a (usually) non-commutative ring.

Definition 6.4. A nonzero element $r \in R$ is called a *zerodivisor* if there exists $s \in R$ such that $rs = 0$. We say r is *nilpotent* if $r^n = 0$ for some $n \in \mathbb{N}$. We say r is a *unit* if there exists $s \in R$ such that $rs = 1$. If such an s exists, it is automatically unique.

Remark 6.5. The units of R are denoted $R^\times$ or R^* . They form an abelian group under multiplication.

There are two notions of sub-object in ring theory.

Definition 6.6. A *subring* of R is an additive subgroup $S \subset (R, +)$ such that $1 \in S$ and S is closed under multiplication.

Definition 6.7. An *ideal* in a ring R is an additive subgroup $I \leq (R, +)$ such that for every $r \in R$ and $x \in I$, $rx \in I$.

Remark 6.8. For an ideal $I \subset R$, $1 \in I$ if and only if $I = R$. More generally, $I = R$ if and only if there is a unit $u \in I$.

Definition 6.9. A *ring homomorphism* between rings R, S is a map $\varphi: R \rightarrow S$ such that $\varphi: (R, +) \rightarrow (S, +)$ is a group homomorphism, $\varphi(1) = 1$, and $\varphi(r)\varphi(r') = \varphi(rr')$ for all $r, r' \in R$.

Remark 6.10. The kernel and image of a ring homomorphism $\varphi: R \rightarrow S$ are defined as usual for the underlying group homomorphism. We have $\ker \varphi$ is an ideal in R and $\text{im } \varphi$ is a subring of S .

Definition 6.11. Given an ideal $I \subset R$, the quotient of the additive groups R/I has a natural induced ring structure defined by

$$r + I \cdot r' + I = rr' + I.$$

The quotient map $q: R \rightarrow R/I$ is a surjective ring homomorphism with kernel I .

Remark 6.12. The quotient ring is the unique ring structure on R/I such that q is a ring homomorphism, and such a structure exists if and only if I is an ideal.

Hence, an additive subgroup $H \leq (R, +)$ is an ideal if and only if there is some ring S and ring homomorphism $\varphi: R \rightarrow S$ such that $H = \ker \varphi$.

Definition 6.13. For a subset $X \subset R$ the *ideal generated by X* is the set

$$(X) = \left\{ \sum_{i=1}^n r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

Definition 6.14. Given ideals $I, J \subset R$, we can construct multiple new ideals:

- i. $I + J := \{a + b \mid a \in I, b \in J\}$
- ii. $I \cap J$
- iii. $IJ = \{\sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J\}.$

Definition 6.15. An ideal I is

- i. *maximal* if it is proper and not contained in any other ideal
- ii. *prime* if $ab \in I$ implies $a \in I$ or $b \in I$
- iii. *principal* if I is generated by a single element a , i.e. $I = (a)$.

Fact 6.16. Maximal ideals are always prime.

Theorem 6.17 (Zorn's Lemma). Suppose $(X, \leq)$ is a poset. If every increasing countable chain has a maximal element, then there exists a maximal element of X .

Exercise 6.18. Every proper ideal is contained in a maximal ideal (by Zorn's lemma).

Definition 6.19. An element $x \in R$ is called *prime* if and only if it generates a (principal) prime ideal.

Definition 6.20. Given R, S rings, the product ring is $R \times S$ with addition and multiplication defined componentwise.

The direct product of rings is also naturally a ring, but the direct sum fails to have a unit.

Lemma 6.21 (Unnamed Lemma). Suppose $\varphi: R \rightarrow S$ is a ring homomorphism and let $I = \ker \varphi$. Then, there exists $\tilde{\varphi}: R/I \rightarrow S$ such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ q \downarrow & \nearrow \tilde{\varphi} & \\ R/I & & \end{array}$$

commutes. It is defined by $\tilde{\varphi}(r + I) = \varphi(r)$.

Theorem 6.22 (Isomorphism Theorems).

- I. If $\varphi: R \rightarrow S$ is a surjective homomorphism and $I = \ker \varphi$, the induced map $\tilde{\varphi}: R/I \rightarrow S$ is an isomorphism.
- II. Let $S \subset R$ be a subring and $I \subset R$ be an ideal. Then, $S + I$ is a subring of R and $S \cap I$ is an ideal in S . Furthermore, the map $S/(S \cap I) \rightarrow (S + I)/I$ defined by $s(S \cap I) \mapsto sI$ is a well-defined isomorphism

$$S/(S \cap I) \cong (S + I)/I.$$

- III. (Lattice Isomorphism Theorem) Suppose I, J are ideals of G and $J \leq I$. Denote by

$$I/J := q_J(I) = \{xJ \mid x \in I\}.$$

This is an ideal in R/J . Furthermore, the map $R/I \rightarrow (R/J)/(I/J)$ defined by $xI \mapsto (xJ)(I/J)$ is a well-defined isomorphism

$$R/I \cong (R/J)/(I/J).$$

- IV. (Correspondence Theorem) Suppose $I \subset R$ is an ideal. Then, there is a bijective correspondence

$$\{\text{ideals of } R \text{ containing } I\} \leftrightarrow \{\text{ideals of } R/I\}$$

given by $\tilde{I} \mapsto \tilde{I}/I$. Furthermore, $\tilde{K}$ is normal in G if, and only if, $\tilde{K}/N$ is normal in G/N .

Definition 6.23. A commutative ring R is *Noetherian* if any of the following equivalent conditions holds:

- i. R satisfies the Ascending Chain Condition: every ascending sequence of ideals $I_1 \subset I_2 \subset \dots$ eventually stabilizes, i.e. there exists n such that $I_n = I_{n+1} = \dots$.
- ii. every ideal in R is finitely generated.

Exercise 6.24. Prove these are equivalent.

7 Integral Domains

Definition 7.1. A commutative ring R is an *integral domain* if it has no zero divisors.

Example 7.2. Fields, $\mathbb{Z}$, $R[x_1, \dots, x_n]$ for R an integral domain.

Example 7.3 (Quadratic Integers). Let $D \in \mathbb{Z}$ be square free. For $D \equiv 2, 3 \pmod{4}$, define $\mathcal{O}_D := \mathbb{Z}[\sqrt{D}]$. For $D \equiv 1 \pmod{4}$, define $\mathcal{O}_D := \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. The reason for the strange definition when $D \equiv 1 \pmod{4}$ comes from the fact that $\mathbb{Z}[\sqrt{D}]$ is not closed under roots of integral monic polynomials in $\mathbb{Q}[\sqrt{D}]$.

These rings are called *quadratic integer rings*.

Fact 7.4. An ideal $I \subset R$ is

- i. prime if and only if R/I is an integral domain
- ii. maximal if and only if R/I is a field.

Definition 7.5. If R is an integral domain, an element $x \in R$ is called *irreducible* (or *indecomposable*) if is not a unit or the product of two non-units.

Example 7.6. Prime integers are irreducible in $\mathbb{Z}$. They are also prime in the ring theoretic sense.

Example 7.7. In $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[x]/(x^2 + 5)$, 2 is irreducible but not prime. The ideal (2) has

$$(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6 \in (2)$$

but neither is in (2). This is because this ring is not a UFD.

Definition 7.8. An *Unique Factorization Domain* (or UFD) is an integral domain such that every element x can be written uniquely (up to a unit) in the form

$$x = u \cdot p_1^{d_1} \dots p_k^{d_k}$$

for u a unit, p_i irreducible.

Fact 7.9. In a UFD, irreducible elements are the same as prime elements.

Fact 7.10. In a UFD, prime ideals are all maximal.

Definition 7.11. A *Principal Ideal Domain* (or PID) is an integral domains such that every ideal is principal.

Example 7.12. $\mathbb{Z}$, $k[x]$ for k a field. $\mathbb{Z}[x]$ is not a PID because of things like $(2, x)$.

Problem (Jan 2025, 2). Let k be a field and let $A = k[X, Y]/(X^2, XY, Y^2)$.

- a. Explicitly determine the invertible elements of A .

- b. Explicitly classify the principal ideals of A .

Problem (Aug 2025, 4). Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(x^2 - y^2)$ are not isomorphic for any field F .

Remark 7.13. All PIDs are Noetherian rings. Remember that PIDs are assumed to be integral domains while Noetherian rings are not!

Trick 7.14. PIDs can be very tricky to work with. A good trick to remember is that the “quotient ideal”

$$(I : a) = \{r \in R \mid ra \in I\}$$

is generated by a single element b . This is like the only place I ever see this ideal.

Problem (Aug 2025, 3). Let R be an integral domain such that every prime ideal of R is principal.

- a. Consider the set of ideals of R which are not principal. Prove that if this set is non-empty, then it contains an element I which is maximal under inclusion.
- b. Prove that R is a principal ideal domain. (Hint: Show that I is principal).

Problem (Jan 2022, 2). a. Let R be an integral domain such that every prime ideal of R is principal. Prove that R is a principal ideal domain.

Hint: consider the set of ideals of R which are not principal. Prove that if this set is non-empty then it contains an element I which is maximal under inclusion.

- b. Prove the $\mathbb{Z}[\sqrt{-3}]$ is not a principal ideal domain.

Problem (Jan 2023, 3). Let A be a PID and let $I_1 \supsetneq I_2 \supsetneq \dots$ be a strictly decreasing sequence of ideals. Prove that $\bigcap_n I_n = (0)$. (You should prove any non-trivial statements about PIDs that you use in this problem.)

Problem (Jan 2024, 3). Let S be a commutative ring. We say a non-invertible $s \in S$ is *indecomposable* if $s = a \cdot b$ for $a, b \in S$ implies at least one of a, b is invertible.

- a. Let S be an integral domain, and $s \in S$ a non-invertible element. Show s is indecomposable if, and only if, (s) is maximal among proper principal ideals (ideals generated by a single non-invertible element).
- b. Show that in a Noetherian integral domain, any element is a product of indecomposable elements.

Trick 7.15. Functions between finite sets of the same size (or linear maps between vector spaces of the same dimension) are injective if and only if they are surjective.

Problem (Aug 2024, 2). a. Prove that a finite integral domain is a field.

- b. Let R be an integral domain with unit element such that $R[x]$ is a principal ideal domain. Prove that R is a field.

Definition 7.16. A *Euclidean Domain* is an integral domain which admits a “norm” $d: R \setminus \{0\} \rightarrow \mathbb{N}$ such that for any elements a, b with $b \neq 0$, there exist q, r satisfying $a = bq + r$ and $r = 0$ or $d(r) < d(b)$.

Example 7.17. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, some other quadratic integer rings.

Theorem 7.18. Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral domains

Problem (Aug 2022, 1). a. Let A be a Euclidean domain with Euclidean function $\delta: A \rightarrow \mathbb{Z}^{\geq 0}$. Show that A is a PID.

- b. Let A be a PID. Show A is a UFD.

- c. Let $d \in \mathbb{Z}$ be an integer congruent to 1 modulo 4. Let $a = \mathbb{Z}[\sqrt{d}]$, and let F denote the field of fractions of A . Show that the polynomial $t^2 - t + \frac{1-d}{4}$ is irreducible in $A[t]$ but is not irreducible in $F[t]$. Deduce that A is not a UFD.

8 Localization

Definition 8.1. Suppose $S \subset R$ is a multiplicative set, i.e. a subset closed under multiplication. Then, we can define a ring $S^{-1}R$ by

$$S^{-1}R = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\} / \sim$$

where

$$\frac{r}{s} \sim \frac{r'}{s'}$$

if and only if $s'r - rs'$ is 0 or a zero-divisor in R .

Example 8.2. For $\mathbb{Z}$, with $S = \mathbb{Z} \setminus \{0\}$, we have $S^{-1}\mathbb{Z} = \mathbb{Q}$.

Example 8.3. If $\mathfrak{p} \subset R$ is a prime ideal, the set $S = R \setminus \mathfrak{p}$ is multiplicative. The resulting ring $S^{-1}R$ is often denoted $R_{\mathfrak{p}}$ and called the *localization* of R at $\mathfrak{p}$. This is because it is a *local ring* (has a unique maximal ideal) and its maximal ideal is $\mathfrak{p}$.

Example 8.4. In the case $\mathfrak{p} = (0)$ is prime, $R_{\mathfrak{p}}$ is a field. This can be very useful for reducing problems about integral domains to problems about vector spaces.

9 Basic Module Theory

Definition 9.1. For R a commutative ring, a (left) R -module is an abelian group M with an action $R \times M \rightarrow M$ denoted by $(r, m) \mapsto r \cdot m$ such that

- i. $r \cdot (x + y) = r \cdot x + r \cdot y$
- ii. $(r + s) \cdot x = r \cdot x + s \cdot x$
- iii. $(rs) \cdot x = r \cdot (s \cdot x)$
- iv. $1 \cdot x = x$.

Example 9.2. For R a field, R -modules are precisely vector spaces.

Example 9.3. For $R = \mathbb{Z}$, R -modules are precisely abelian groups.

Definition 9.4. A *submodule* is a subset $N \subset M$ closed under addition and scalar multiplication by R .

Definition 9.5. A *module homomorphism* between R -modules M, M' is a group homomorphism $\varphi: M \rightarrow M'$ such that $\varphi(r \cdot x) = r \cdot \varphi(x)$.

Fact 9.6. The kernel and image of a module homomorphism are submodules of the domain and codomain, respectively.

Definition 9.7. The *annihilator* of a module M is the ideal $\text{Ann}(M) \subset R$ defined

$$\text{Ann}(M) = \{r \in R \mid rx = 0 \forall x \in M\}.$$

An element $r \in R$ is said to *annihilate* $m \in M$ if $r \cdot m = 0$.

Definition 9.8. The *torsion submodule* of a module M is the set of *torsion elements*, i.e. $m \in M$ annihilated by some non-zero-divisor of R .

Definition 9.9. An R -module M is called

- i. *simple* if it contains no proper nontrivial submodules
- ii. *finitely generated* if there exist finitely many elements such that every element in M is an R -linear combination of them
- iii. *cyclic* if M is generated by a single element
- iv. *free* if M is isomorphic to the direct sum module R^I for some index set I
- v. *indecomposable* if M cannot be written as the direct sum of two submodules.
- vi. *torsion-free* if its torsion submodule is trivial.

Problem (Jan 2024, 4). Let S be a commutative integral domain. Suppose every finitely generated torsion-free S -module is free. Prove that S is a PID.³

Fact 9.10. Any module homomorphism between simple modules is either an isomorphism or 0.

Trick 9.11. One trick when working with R -modules is to quotient by a maximal ideal and pass to a problem about vector spaces.

Problem (Aug 2024, 3). Show that if the free R -modules R^n and R^m over a non-zero commutative ring R are isomorphic, then $n = m$. Is this true if R is non-commutative?

10 Modules over PIDs

Example 10.1. An easy ring to consider modules for is $k[t]$, for k a field. Any $k[t]$ -module is necessarily a k -module, hence a vector space V . Then, the data of a $k[t]$ -module is precisely a question of how t acts on the vector space. Because t commutes with scaling by k and distributes over addition, t must act by an element of $GL(V)$.

Problem (Aug 2023, 1a). Let L be a field, $V := L^n$ the L -vector space of column vectors with n entries, and $R := L[T]$ the ring of polynomials with coefficients in L .

- i. Explain why an R -module structure on V , restricting to its natural L -module structure, determines and is determined by an $n \times n$ matrix over L .
- ii. For an $n \times n$ matrix A , let V_A be the corresponding R -module. Show that V_A and V_B are isomorphic if, and only if, the matrices A, B are conjugate.

Problem (Jan 2022, 3). Consider the 2-dimensional $\mathbb{R}$ -vector space $V = \mathbb{R}^2$, the linear transformation $T_1: V \rightarrow V$ which is the projection onto the y -axis, and the linear transformation T_2 induced by the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Then, view V as an $\mathbb{R}[x]$ -module V_i where $x \cdot v = T_i(v)$.

Describe the $\mathbb{R}[x]$ -module structure of V_i for $i = 1, 2$. Determine whether V_1 and V_2 are isomorphic as $\mathbb{R}[x]$ -modules.

Theorem 10.2 (Smith Normal Form). Let A be a nonzero $m \times n$ matrix in a PID R . There exist invertible $m \times m$ and $n \times n$ matrices S, T such that

$$SAT = \text{diag}(\alpha_1, \dots, \alpha_r, 0, \dots, 0)$$

where

$$\alpha_i = \frac{d_i(A)}{d_{i-1}(A)}$$

up to a unit, for $d_i(A)$ the gcd over all determinants of $i \times i$ minors in A . The α_i are called invariant factors and satisfy $\alpha_i \mid \alpha_{i+1}$. They are unique up to a unit.

³As written, this problem is false; one can show that every finitely generated ideal in S is principal, but there exist rings with this property with non finitely generated non principal ideals.

Example 10.3. For a 2×2 matrix, the Smith Normal Form of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\text{diag}(d_1, d_2/d_1)$ with $d_1 = \gcd(a, b, c, d)$ and $d_2 = |ad - bc|$.

Example 10.4. In the case that R is a field, every α_i is a unit, and r is simply the rank of the matrix.

Remark 10.5. When R is not a field, the Smith normal form is essentially telling us how far away the cokernel (codomain mod image) is from being free. In particular, we have

$$R^m / \text{im}(A) \cong R/(\alpha_1) \oplus \cdots \oplus R/(\alpha_r).$$

Problem (Jan 2025, 3). a. Find the invariant factors of the quotient group $\mathbb{Z}^3/N$, where N is the subgroup of $\mathbb{Z}^3$ generated by $(-4, 4, 2)$, $(16, -4, -8)$, and $(8, 4, 2)$.

b. Let $\mathbb{F}_2$ be the field of 2 elements and let $R = \mathbb{F}_2[X]$. List up to isomorphism all R -modules with exactly 16 elements.

11 Linear Algebra

There are a few major theorems from linear algebra worth remembering.

Definition 11.1. The characteristic polynomial of a matrix $A \in M_n(K)$ is

$$\chi_A(\lambda) = \det(A - \lambda \text{id}).$$

Its zeros are the eigenvalues of A , numbers λ such that for some $v \in K^n$ we have $Av = \lambda v$ (called an eigenvector with eigenvalue λ).

Theorem 11.2 (Cayley-Hamilton). Any matrix is a zero of its own characteristic polynomial, i.e. $\chi_A(A) = 0$.

Definition 11.3. The minimal polynomial of a matrix $A \in M_n(K)$ is the polynomial m_A of minimal degree such that $m_A(A) = 0$.

Remark 11.4. $m_A \mid \chi_A$, but they are not always equal.

Problem (Jan 2025, 4). Does there exist a 3×3 matrix A over $\mathbb{Q}$ such that $A^8 = I$ but $A^4 \neq I$?

Definition 11.5. A matrix is *diagonalizable* if and only if it has a basis of eigenvectors. Equivalently, A is similar to a diagonal matrix, i.e. $A = XDX^{-1}$ for $X \in GL_n(K)$ and D diagonal.

Example 11.6. The matrix

$$\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$$

is a canonical example of a non-diagonalizable matrix.

Fact 11.7. A matrix is diagonalizable if and only if its minimal polynomial has no repeated roots.

Theorem 11.8 (Jordan Normal Form). If the characteristic polynomial of A has all of its roots in K , then A is conjugate to a block-diagonal matrix of the form

$$\begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & J_k \end{bmatrix}$$

where each J_i is of the form

$$\begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{bmatrix}$$

Example 11.9. A matrix whose characteristic polynomial splits with all unique eigenvalues is necessarily diagonalizable.

Problem (Jan 2023, 2). Let $t \in M_n(\mathbb{C})$ be an $n \times n$ -matrix such that T^r equals the identity matrix for some integer $r \geq 1$. Prove that T is conjugate to a diagonal matrix.

Problem (Aug 2023, 2b). A finite group is not the union of conjugates of any proper subgroup. Show by way of example that this fails in general for infinite groups. Equivalently, give an example of a proper subgroup H of a group G such that every element of G is conjugate to an element of H .

Theorem 11.10 (Rational Canonical Form). Let K be any field. Suppose $A \in M_n(K)$. Let $\text{diag}(d_1, \dots, d_n)$ be the Smith normal form of $A - xI \in M_n(K[x])$, with $d_1 \mid d_2 \mid \cdots \mid d_n$ (with d_i possibly 0 for all $i > r$ for some r). For each $d_i \in K[x]$, form the companion matrix

$$C(d_i) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

Then, A is similar (over $GL_n(K)$) to a block diagonal matrix of the form $\text{diag}(C(d_1), \dots, C(d_n))$.

Problem (Aug 2023, 1b). Let $L \subset K$ be a field extension. Let A, B be $n \times n$ matrices over L which are conjugate over K . Are they necessarily conjugate over L ? If so, prove it; if not, give a counterexample.

12 Other

Problem (Aug 2025, 2). Show that for G a finite abelian group, any irreducible n -dimensional complex representation is one-dimensional.