M373K Lecture Notes

Lewis Bowen*
University of Texas at Austin

March 18, 2013

Contents

1 3/19/13: A few reminders **1**

2 Subrings of $\mathbb{C}$ **1**

3 Rings! **2**
3.1 A brief look forward 3
3.2 Kinds of rings 3
3.3 finite characteristic 3
3.4 homomorphisms 4
3.5 Example 5
3.6 Maximal ideals 5

1 3/19/13: A few reminders

Sukhpreet Singh's office hours: TTh 3:15-4:15. RLM 12.120.

I should return homeworks.

There is a homework due on Thurs.

Exam 2 is on Thurs 3/28. I will make a practice sheet. It will cover chapter 2.

2 Subrings of $\mathbb{C}$

Any subset of $\mathbb{C}$ that is closed under multiplication, addition and subtraction is a subring of $\mathbb{C}$. For example $\mathbb{Z}[i]$ are the Gaussian integers. $\mathbb{Z}[\sqrt{2}]$ consists of all elements of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$.

*email:lpbowen@math.utexas.edu

3 Rings!

Examples:

- The integers;
- The integers modulo n;
- $Mat(n)$,
- Any subset of $\mathbb{C}$ that is closed under multiplication, addition and additive inverses. For example, $\mathbb{Z}[i]$, $\mathbb{Z}[1/2], \mathbb{Z}[\sqrt{2}], \mathbb{Q}[\sqrt{2}]$, etc.
- The polynomial rings $\mathbb{C}[X], \mathbb{C}[X, Y]$, etc.
- bounded linear operators on a Hilbert space;
- $C(X)$, the ring of continuous functions on a space X
- the quaternions;
- algebra of observables in a quantum mechanical system, algebra of continuous functions on a topological space.
- $\mathbb{Z}G$.

Definition: a *ring* is a set R with two binary operations $+, \times : R \times R \to R$ such that

- $(R, +)$ is an abelian group.
- $\times$ is associative.
- the distributive laws holds: $a \times (b + c) = ab + ac$, $(b + c)a = ba + bc$.

Remarks and notation

1. the additive identity is denoted by 0. So $a + 0 = a = 0 + a$ for every $a \in R$.
2. The additive inverse of an element a is denoted by $-a$.
3. There does not have to be a multiplicative identity. For example, $2\mathbb{Z}$ is a ring. However, if there is a multiplicative identity, it is denoted by 1 and in this case the ring is called a *unital ring* or *ring with unit*.
4. It is common practice to denote $1 + 1$ by 2 and $1 + 1 + 1$ by 3, etc. We do this even if $3 = 0$ in R. For example, $\mathbb{Z}/3\mathbb{Z}$ is a ring.
5. Claim: for any $a \in R$, $(a + a + a + \cdots + a) = na$. Proof: the latter is the same as $(1 + 1 + \cdots + 1)a$ by the distributive property. Note that $na = an$ if n is an integer.
6. If $ab = ba$ for every $a, b \in R$ then R is *commutative*.

Lemma 3.1. *If $a \in R$ then $a0 = 0$.*

Proof. $a(0 + 0) = a0 = a0 + a0$. So $a0 = 0$. □

3.1 A brief look forward

1. Kind of rings and basic properties
2. homomorphisms, ideals, quotient rings;
3. prime factorization, its analogs in other rings
4. polynomial rings and subrings of $\mathbb{C}$.

3.2 Kinds of rings

1. A ring is *unital* if it has a multiplicative identity;
2. A ring is *commutative* if ab=ba for avery $a, b \in R$;
3. A nonzero element $a \in R$ is a *zero-divisor* if there is a nonzero element b such that $ab = 0$. Which rings have zero divisors?
4. If R is commutative and has no zero-divisors then R is an *integral domain*.
5. If every nonzero $a \in R$ has a multiplicative inverse then R is a *division ring* or *skew field*.
6. If $(R \setminus \{0\}, \times)$ is an abelian group then R is a *field*.

Note

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

So $Mat(2)$ has zero divisors. Does $\mathbb{Z}/6\mathbb{Z}$ have zero divisors?

The quaternions are a division ring but not a field.

There are a lot of interesting fields: $\mathbb{Z}/p\mathbb{Z}$, subfields of $\mathbb{C}$, the field of rational functions $\mathbb{C}(X)$, ...

Good problems: 3.2: 1, 5, 6, 10.

The three main ideas in group theory are subgroups, quotient groups and homomorphisms. We will see similar ideas in ring theory.

3.3 finite characteristic

Definition 1. An integral domain R has characteristic m if $(1 + 1 + \cdots + 1) = 0$ in R. In other words, if $m = 0$ in R. If there is no such m then we say R has characteristic 0.

Example: $(\mathbb{Z}/p\mathbb{Z})$ has characteristic m. The integers have characteristic 0.

Is $(\mathbb{Z}/p\mathbb{Z})[X]$ an integral domain? Yes and its characteristic is p.

Lemma 3.2. *If a finite integral domain has characteristic $p \neq 0$ then R is a field.*

Proof. Let $a \in R$ be nonzero. Let $\phi : R \to R$ be the map $\phi(r) = ar$. We claim ϕ is 1-1. Indeed, if $\phi(r) = \phi(s)$ then $ar = as$. So $\phi(r - s) = a(r - s) = ar - as = 0$. However, R is an integral domain and $a \neq 0$. So $r - s = 0$ which implies $r = s$. So ϕ is 1-1. Because R is finite, ϕ must be a bijection. So there exists r such that $\phi(r) = a$. In other words, $ar = a$. We claim that r is a multiplicative identity. If $b \in R$ then there exists $c \in R$ such that $\phi(c) = b = ac = ca = car = br$. So $b = br = rb$ as required.

Now let $d \in R$ be such that $\phi(d) = 1$ which means $ad = 1$ which means $d = a^{-1}$. □

3.4 homomorphisms

Defn: A *homomorphism* is a map $\phi : R \to R'$ from one ring to another such that

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$. An isomorphism...

In this case, $\phi(0) = 0$ and $\phi(-a) = -\phi(a)$.

A homomorphism is 1-1 iff the kernel is $\{0\}$.

Definition 2. The *kernel* of ϕ is the set I of all element $r \in R$ such that $\phi(r) = 0$. Observe that I is closed under addition and if $a \in I, r \in R$ then $ar, ra \in I$. Any subset of R with these properties is called a *two-sided ideal*.

Examples:

1. the zero homomorphism
2. the identity homomorphism
3. $\mathbb{Z}$ onto $\mathbb{Z}/n\mathbb{Z}$;
4. $\mathbb{Z}[X]$ to $\mathbb{C}$ the evaluation map of a polynomial.
5. $C(\mathbb{R})$ to $\mathbb{R}$ the evaulation map at a point.
6. the conjugation map from $\mathbb{C}$ to itself,
7. the selfmap of $\mathbb{Z}[\sqrt{2}]$ which takes $a + \sqrt{2}b$ to $a - \sqrt{2}b$.
8. the map from $\mathbb{Q}[x]$ to $\mathbb{C}$ given by $f \mapsto f(\pi)$. What's the kernel? (It's 0 so this is an isomorphic embedding). This is because π does not satisfy any polynomial with rational coefficients.

Given a ring R and a 2-sided ideal I we define the *quotient ring* R/I: its additive structure is the same as the quotient additive structure that is R/I consists of all cosets $a + I$ of I in R as an abelian group. The multiplicative structure is defined by $(a + I) \times (b + I) = ab + I$.

Is this well-defined? Is $ab + I = (a + I)(b + I)$ as sets?

Let's handle the second question first. By the distributive laws $(a+I)(b+I) = ab+Ib+aI+I^2$

Example: if $R = \mathbb{Z}, I = n\mathbb{Z}$ then we have $(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+bn\mathbb{Z}+an\mathbb{Z}+n^2\mathbb{Z} = ab+gcd(bn,an,n^2)\mathbb{Z}$. So this doesn't work (choose $a=b=n=2$). The problems is that $I^2 \neq I$.

Let's handle the first question now. If $a+I = a'+I, b+I = b'+I$ then there exist $r,s \in I$ such that $a' = a+r, b' = b+s$. So

$$a'b'+I = (a+r)(b+s)+I = ab+rb+as+rs+I = ab+I$$

since $rb, as, rs \in I$. So it is well-defined.

One can check that this does define a ring. Of course there is a canonical homomorphism from R to R/I.

3.5 Example

Define $\phi : \mathbb{Z}[x] \to \mathbb{C}$ by $\phi(f) = f(i)$ where i is the complex unit.

Observe that the kernel I of ϕ consists of all polynomials $f(x)$ such that $f(i) = 0$. By the fundamental theorem of arithmetic this is equivalent to stating that $f(x)$ is divisible by x^2+1. In other words, $I = (x^2+1)$ is the smallest ideal containing x^2+1.

Therefore the image of ϕ is isomorphic to $\mathbb{Z}[x]/(x^2+1)$. Suppose that $g \in \mathbb{Z}[x]$. Then $g = qf+r$ for polynomials q, r with $deg(r) < deg(f) = 2$ by the division algorithm. Therefore $g+I = r+I$. So every element of $\mathbb{Z}[x]/(x^2+1)$ can be written as $ax+b+I$ for some $a,b \in \mathbb{Z}$. Now ϕ induces a homomorphism $\phi' : \mathbb{Z}[x]/(x^2+1) \to \mathbb{C}$ by $\phi'(ax+b+I) = ai+b$. This has no kernel and is onto $\mathbb{Z}[i]$. So $\mathbb{Z}[x]/(x^2+1)$ is isomorphic to $\mathbb{Z}[i]$.

Can you work out a similar example with $\mathbb{Z}[\sqrt{2}]$? How about $\mathbb{Z}[\frac{\sqrt{3}}{2}+(1/2)i]$?

Exercise: show that $\mathbb{Z}[X]/(f)$ is isomorphic to the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and all roots of f assuming f is irreducible over $\mathbb{Q}$.

3.6 Maximal ideals

Lemma 3.3. *If R is a commutative ring with unit and its only ideals are R and (0) then R is a field.*

Remark 1. This doesn't hold if R is non-commutative. Example: the ring of matrices has no nontrivial ideals.

Definition 3. An ideal $I \subset R$ is maximal if $I \neq R$ and if J is any ideal with $I \subset J \subset R$ then either $J = I$ or $J = R$.

examples

1. $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, $10\mathbb{Z}$ is not. IMPORTANT CONNECTION: maximal ideals and primes.

2. (x^2+1) is not a maximal ideal in $\mathbb{Z}[x]$ because $(x^2+1, 3)$ contains it. In fact, $\mathbb{Z}[x]/(x^2+1, 3) \approx \mathbb{Z}[i]/(3)$ is a field of order 9. Indeed, the inverse of $1+2i$ is $(a+bi)$ where $a-2b \equiv 1 \mod 3$, $2a+b \equiv 0 \mod 3$. Since $-2 \equiv 1$ this is $a+b \equiv 1, 2a+b \equiv 0$ which implies $2b \equiv 1$ which implies $b = 2$ which implies $a = 2$. So $(1+2i)(-1-i) = 1-3i$. $(2+2i)(1+2i) = (-2+6i) \equiv -2$....

3. The set of functions which take 0 to 0 in $C(\mathbb{R})$ is maximal.

Lemma 3.4. *If R is a commutative ring with unit and I is an ideal then R/I is a field iff I is maximal.*