Algebra

Evan Fox

September 11, 2022

Chapter 1

Rings

1.1 Integral domains and division rings

Definition 1.1.1
Let R be a set and define $+ : R \times R \to R$ denoted $(a, b) \mapsto a + b$ and $\cdot : R \times R \to R$ denoted $(a, b) \mapsto ab$ and assume

1. *$(R, +)$ is an abelian group*
2. *$(R, \cdot)$ is associative and closed*
3. *$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$*

Then R is a ring.

If the multiplication on R is communitive then we say that R is a communitive ring. Note in general there need not exist $1 \in R$ satisfying $1 \cdot a = a$ for all $a \in R$, since $(R, \cdot)$ is not necessarily a group. An informal way of defining a ring is just to consider a set where addition, subtraction, and multiplication make sense.

Remark 1.1.2
Let R be a ring, for $a, b \in R$ we have

1. *$0b = 0$*
2. *$(-a) \cdot b = -(a \cdot b)$*
3. *$(-a) \cdot (-b) = ab$*

Proof. For the first statement note

$$0b = (0+0)b = 0b = 0b + 0b$$

since R is a group under addition we may make full use of the cancelation property which gives $0 = 0b$. Next observe,

$$(-a)b + ab = ((-a) + a)b = 0b = 0$$

so that ab is the additive inverse of $(-a)b$. The proof of the last result is simillar.

□

The definition of a ring is very general, some classic examples are the integers (mod n), matrices, and continous functions. Showing these are rings is easy.

Remark 1.1.3
Let R be a ring and S a non-empty set. Recall R^S denotes the set of functions $f : S \to R$. Give a addition and multiplication that turns R^S into a ring such that if $|S| = 1$ we have $R^S \sim R$.

Proof. exercise. □

Now we will introduce a very important type of ring called an integral domain. First we must consider the concept of a zero divisor.

Definition 1.1.4
Let R be a ring and $a \in R$ with $a \neq 0$. If there exists non-zero $b \in R$ such that $ab = 0$, then a is a zero divisor.

Definition 1.1.5
Integral Domain A ring R is an integral domain if

1. *R is communitive and $1 \in R$.*
2. *R has no zero divisiors.*

An obvious example of an integral domain is the integers. One can show that that the deffinition of an integral domain is equivalent to a communitive ring where multiplicitive cancelation holds.

Proposition 1.1.6
Let R be a communitive ring, then R is an integral domain iff $ab = ac \implies b = c$ for all $a, b, c \in R$ with a non-zero.

Proof. For the first direction assume that R is an integral domain and let $a \neq 0, b, c \in R$ satisfy $ab = ac$. Then

$$ab - ac = 0 \implies a(b - c) = 0$$

and since a is non zero and R has no zero divisiors we have $b - c = 0$ so $b = c$.

Conversly, assume that the cancellation property holds in R. We need to prove that $ab = 0$ implies $a = 0$ or $b = 0$; so it is sufficient to assume $ab = 0$ and that $a \neq 0$ and show $b = 0$. We know that

$$ab = a0 = 0$$

and the cancellation property shows that $b = 0$. □

Definition 1.1.7
A ring R (not necessarily communitive) is a division ring if $(R^*, 0)$ is a group

If R is a communitive division ring then we say that R is a field. Common examples of fields are $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. A more exotic example is the quadradic field $\mathbb{Q}(\sqrt{D}) :- \{a+b\sqrt{D} | a, b \in \mathbb{Q}\}$ where D is a non-square rational number. The proof that this is a field is left as an exercise.

Theorem 1.1.8
A finite integral domain is a field.

Proof. Let R be a finite integral domain and let $x_1, ..., x_n$ be a list of all elements. Fix $a \neq 0 \in R$ and consider the list

$$S = ax_1, ..., ax_n$$

Since R is an integral domain if there exists $i, j \in \{1, ..., n\}$ such that $ax_i = ax_j$ we have

$$a(x_i - x_j) = 0 \implies x_i = x_j.$$

Hence every element in S is distinct, then since the lenght of S is the same as the cardinality R we see that every element of R appears in S. Cleary a appears in this list, hence there must exist x_{j_0} such that $ax_{j_0} = a$. Now note that for any $r \in R$ we can write $r = ax_k$ and

$$rx_{j_0} = ax_{j_0}x_k = ax_k = r$$

so x_{j_0} is the unit of R. Now we must find the multiplicative inverse of a, since $x_{j_0} \in R$ it appears in S. Hence there exist $X_{i_0} \in R$ such that $ax_{i_0} = x_{j_0}$; it follows that every non zero element of R has a multiplicitive inverse. Thus R is a field □

The above theorem is clearly false in the infinite case (consider the integers), however an interesting note is where the above proof breaks down. In the finite case the function $\cdot_a : R \to R$ defined by $r \mapsto a \cdot r$ is an injective mapping from R to R and is then necessarily a bijection. However for sets with infinite cardinality, you can have a injective map from a set to inself that is not surjective; and this is where the logic of the above breaks down.

A field is a very important structure in mathematics and we will have much more to say about them later.

1.2 Ideals and Quotients

In group theory we had subgroups, to extend this to rings we simply require clousure of multiplication.

Definition 1.2.1
Let R be a ring and suppose $S \subseteq R$. We say S is a subring og R if

1. *S is a subgroup of R when considered under addition*
2. *S is closed under multiplication*

We may want to test wether or not a given subset is a subring, here we show a way of doing that (we have basicaly just stolen the subgroup test.)

Theorem 1.2.2 (Subring test)
$S \subseteq R$ is a subring if

1. *$a, b \in S \implies a - b \in S$ and $ab \in S$*

Proof. exercise □

We will find that the concept of subrings is not so important. What we really want to study are the ideals of a ring. In group theory we found the concept of a normal subgroup to be extremly usefull, so it is natural to ask if we can produce a similar concept for rings such that we may bring over many of our previous results. If we consider R as a group it is clear that every subgroup is normal (since R is abealian), but what should we require of multiplication? We will soon see that the next deffinition is the correct one.

Definition 1.2.3 (Ideals of a ring)
Let R be a ring. A (two-sided) ideal of R is a subring U such that for all $r \in R$ and all $u \in U$ $ru \in U$ and $ur \in U$.

Remark 1.2.4
Technically we may speak of left ideals and right ideals, were U would only be closed under multiplication on the left or right, this is why we must add the condition of a two sided ideal. In these notes we will only consider the notion of two sided ideals. Note in a communitive ring a left and right ideal concided and there is no difference.

Now given an ideal U we know that the cosets $a + U$ for all $a \in R$ partition R and we know how to turn $R\backslash U$ into a group. Now we need to define a multiplication on $R\backslash U$ to turn it into a ring. Obviously we would like

$$(a + U)(b + U) = (ab) + U$$

lets show that our defintion of ideal ensures that this will work

Proposition 1.2.5
$R\backslash U = \{a + U | a \in R\}$ *with the above operations is a ring*

Proof. we must show that the definition of multiplicatin is well defined. Let $a, a', b, b' \in U$ and assume $a + U = a' + U$ and $b + U = b' + U$. We need to show that

$$(ab) + U = (a'b') + U$$

Note $a \in a + U$ so $a = a' + u_s$ and the same argument shows $b = b' + u_t$ for $u_s, u_t \in U$. Now for $x \in (ab) + U$ we have

$$x = ab + u_1 = (a' + u_2)(b' + u_3) + u_1$$

$$= a'b' + a'u_3 + u_2b' + u_2u_3 = a'b' + u_4 \in (a'b') + U.$$

Which shows $(ab) + U \subseteq (a'b') + U$. The converse is simillar and this completes the proof.

□

Hence multiplication works as expected. The above proof also makes clear why we defined ideals the way we did. Now we move on to consider two more types of ideals, prime ideals and maximal ideals.

Definition 1.2.6 (Prime Ideals)
Let I be an ideal of a ring R, we say I is a prime ideal if all $a, b \in R$ we have $ab \in I$ implies $a \in I$ or $b \in I$.

Prime ideals get there name from the ideals $p\mathbb{Z} \subseteq \mathbb{Z}$. An easy exercise is to show that for all prime p, $p\mathbb{Z}$ is prime.

Definition 1.2.7 (Maximal Ideals)
Let M be an ideal. We say that M is maximal if $M \subseteq U \subseteq R$ implies $M = U$ or $M = R$.

An ideal is maximal when it is impossible to fit another ideal between it and the entire ring.

We imeaditly see two results

Theorem 1.2.8
I is a prime ideal of a ring R iff $R\backslash I$ is an integral domain

Proof. Suppose that I is a prime ideal then $(a+I)(b+I) = I = (ab) + I$ hence a or b is in I so either $(a+I) = I$ or $b + I = I$. Conversly let R be a ring and I an ideal. Now suppose $R\backslash I$ is an integral domain. Now assume $ab \in I$. Then $I = (ab) + I = (a+I)(b+I)$ and since $R\backslash I$ is an integral domain one of $a+I$ or $b+I$ must equal I and it follows from this that either $a \in I$ or $b \in I$. □

For maximal ideals we see an even stronger result, but first we prove a lemma.

Lemma 1.2.9
Let k be a communitive ring with unit. Then k is a field if and only if the only ideals of k are the trivial ring and k itself.

Proof. Assume k is a field and U a non trival ideal. Then for $a \neq 0 \in U$ and $a^{-1}, x \in k$ we have

$$a(a^{-1} \cdot x) = 1 \cdot x = x \in U$$

so $k = U$. Conversly, assume k is a communitive ring whose only ideals are trivial and k itself. For $a \neq 0 \in k$ we have the non trival ideal $\langle a \rangle = \{ar | r \in k\}$, by assumtion this ideal must necessarily be k itself, in particular it must contain 1. But this means there exist $b \in k$ with $ab = 1$. Since a was an arbitrary non zero element we have that k^* is an abelian group and from this the result follows. □

Theorem 1.2.10
M is a maximal ideal if and only if $R\backslash M$ is a field.

Proof. Consider the map $\phi : R \to R\backslash M$ defined by $r \mapsto r + M$. Now let U be an ideal containg M then

$$\phi(U) = \{u + M | u \in U\}$$

Since $M \subseteq U$ we know $M \in \phi(U)$. Now for $a, b \in U$ we have $a+M, b+M \in \phi(U)$ so

$$a + M - b + M = (a - b) + M \in \phi(U)$$

since $a - b \in U$. Now for $r \in R$ we have $r + M \in \phi(R)$ and

$$(a + M)(r + M) = (ar) + M \in \phi(U)$$

hence $\phi(U)$ is an ideal of $R\backslash M$. Now consider an ideal of $R\backslash M$, say I. Then $\bigcup I$ is an ideal of R which maps to I under ϕ. Hence there is a one to one corospondence between ideals of R containg M and ideals in $R\backslash M$. M maps to the trivial ideal and R maps to $R\backslash M$. So then if M is maximal the only ideals of $R\backslash M$ are trivial and itself, so it is a field. If $R\backslash M$ is a field, then the only ideals contain M are M and R, so M is maximal.

□

The previous two theorems show that a maximal ideal is always prime. The converse does not hold in an arbitrary ring however. For example $3\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$ but is not maximal. Infact one can prove that if R is a ring and I a prime ideal then $I[x]$ is a prime ideal of $R[x]$ but this does not hold for maximal ideals.

1.3 Ring Homomorphism

In group theory we found the concept of a homomorphism to be very useful, so we will define the obvious extension to rings.

Definition 1.3.1
Let R and S be rings. A function $\phi : R \to S$ is a ring homomorphism if

1. $\phi(a + b) = \phi(a) + \phi(b)$.
2. $\phi(ab) = \phi(a)\phi(b)$.

just like in group theory, we say that to rings are isomorphic if there exists a bijective homomorphism between them. It is clear that every ring homomorphism is a group homomorphism if we consider the rings as groups and so our knowelge of group homomorphism carrys over. If R, S both have a uinty, then $\phi(1_R) = 1_S$. It follows that if R is a ring with unity, then no homomorphic image of R is a ring without unity.

1.4 PID and UFD

In this section we explore the relation ship between principal ideal domains and unique factorization domains.

Proof. Let $a \in R$ be a nonzero nonunit. We first show that a has a irriducible factor, if a is irriducible we are done so suppose not. Then a must be reducible so we can write $a = a_1 b_1$. where a_1, b_1 are both nonunits. we can repeat the same argument on a_1 to produce

$$a = a_1 \cdot b_1$$

$$a_1 = a_2 \cdot b_2$$

$$a_2 = a_3 \cdot b_3$$

$$.$$

$$.$$

$$.$$

Then $a_{n+1} | a_n$ and $\langle a_n \rangle \subset \langle a_{n+1} \rangle$. Then since PIDs are noetherian, this chain of ideals must become constant for some a_m. Then a_m must be an irriducible factor of a. We relable $a_m = p_1$ and write $a = p_1 \cdot c$. c must be a nonunit lest we have a contradiction on our assumtion on a, so we can repeat the above process on c to obtain an irriducible factor of c, hence $a = p_1 p_2 c_1$ and $\langle c \rangle \subset \langle c_1 \rangle$. Iterating as above gives

$$a = p_1 \cdot p_2 \cdot ... \cdot c_k$$

where $\langle c_k \rangle = \langle c_{k+i} \rangle$. Thus c_k must be irriducible since reduciblity would furnish an ideal proplery containg c_k. This completes the existence portion of the argument.

□