Math 361 lecture for Wednesday, Week 1

Rings

This lecture will be a summary of the basic theory of rings required for this course. Do not be discouraged if you cannot absorb all of the information at once. These are concepts you will gradually understand by working with myriad examples throughout this course. You are already familiar with many rings: the ring of integers, $\mathbb{Z}$; polynomial rings, e.g., $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x, y, z]$; quotient rings such as $\mathbb{Z}/n\mathbb{Z}$; and any field, e.g., $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. A (nonzero) ring is just a field except that nonzero elements are not required to have multiplicative inverses. For example, $2 \in \mathbb{Z}$ has no multiplicative inverse in $\mathbb{Z}$. Check each concept introduced below against the rings you already know.

Definition 1. A *ring* is a set R with two operations, addition $+\colon R \times R \to R$ and multiplication $\cdot\colon R \times R \to R$ satisfying the following axioms:

A1. $a + b = b + a$ for all $a, b \in R$ (commutativity of addition).

A2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ (associativity of addition).

A3. There exists and element $0 \in R$ such that $a + 0 = a$ for all $a \in R$ (additive identity).

A4. For each $a \in R$ there exists an element $b \in R$ such that $a + b = 0$ (additive inverses) [The element b is denoted $-a$. We then define *subtraction* by $x - y := x + (-y)$ for all $x, y \in R$.]

(In the following, we follow the usual convention of writing ab for $a \cdot b$.)

M1. $ab = ba$ for all $a, b \in R$ (commutativity of multiplication).

M2. $a(bc) = (ab)c$ for all $a, b, c \in R$ (associativity of multiplication).

M3. There exists an element $1 \in R$ such that $a1 = a$ for all $a \in R$ (multiplicative identity).

D. For all $a, b, c \in R$, we have $(a + b)c = ac + bc$.

Properties A1–A4 say that R is an *abelian group* under addition. So a ring satisfies all of the field axioms except we do not require $1 \neq 0$ and we do not require that nonzero elements have multiplicative inverses. (Check that if $1 = 0$, then the ring only has one element.) There are also useful noncommutative rings in which we do not require that multiplication is commutative. What we have called a ring is sometime called a *commutative ring with unity*.

Definition 2. An *integral domain* is a nonzero commutative ring with no zero divisors. In other words, $1 \neq 0$ and if $a, b \in R$ with $ab = 0$, then either $a = 0$ or $b = 0$.

Exercise 3. The ring $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain. What are its zero divisors? What are the zero divisors in $\mathbb{Z}/n\mathbb{Z}$ for arbitrary n? When is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?

Exercise 4. The *cancellation law* holds in an integral domain. Let a, b, c be elements in an integral domain R. Show that if $ab = ac$ and $a \neq 0$, then $b = c$.

Ideals

Definition 5. A nonempty subset I of a ring R is an *ideal* if

1. I is closed under addition, and
2. if $r \in R$ and $a \in I$, then $ra \in I$.

Definition 6. An ideal I in a ring R is *generated by* $a_1, \ldots, a_n \in R$ if every element of I is an R-linear combination of elements of $a_1, \ldots, a_n$, i.e., for all $a \in I$, we can write

$$a = \sum_{i=1}^{n} r_i a_i$$

for some elements $r_i \in R$. We then write

$$I = (a_1, \ldots, a_n).$$

We say I is a *principal ideal* if it can be generated by a single element, i.e., if there exists $a \in R$ such that $I = (a) = \{ra : r \in R\}$, all multiples of a single element a of R.

Definition 7. An integral domain R in which every ideal is principal is called a *principal ideal domain*, abbreviated PID.

Definition 8. An ideal I in a ring R is *maximal* if $I \neq R$, and the only ideal of R properly containing I is R, itself. In other words, if J is an ideal of R and $J \supsetneq I$, then $J = R$.

Exercise 9. An ideal I in a ring R is maximal if and only if R/I is a field.

Homomorphisms

Definition 10. A mapping $\phi\colon R \to S$ between rings R and S is a *(ring) homomorphism* if it preserves the ring operations, i.e., for all $a, b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

In that case, the *kernel* of ϕ is

$$\ker(\phi) := \{r \in R : \phi(r) = 0\},$$

and the *image* of ϕ is

$$\operatorname{im}(\phi) := \phi(R) := \{\phi(r) : r \in R\}.$$

The homomorphism ϕ is an *isomorphism* if it is bijective.

Note: "kernal" is a common misspelling of the word "kernel".

Exercise 11. Let $\phi : R \to S$ be a ring homomorphism.

1. $\phi(0) = 0$ (where we are being sloppy with notation: the first 0 is the additive identity of R and the second is the additive identity of S).
2. The kernel of ϕ is an ideal of R.
3. The image of ϕ is not necessarily an ideal of S.
4. ϕ is injective if and only if $\ker(\phi) = \{0\}$.
5. ϕ is an isomorphism if and only if its kernel is trivial (i.e., equal to $\{0\}$) and its image is S.
6. If ϕ is bijective, its inverse (as a mapping of sets) is necessarily a ring homomorphism.

Quotient rings

Definition 12. Let I be an ideal in a ring R. The *cosets* of I are the sets of the form $a+I := \{a+i : i \in I\}$ for each $a \in R$. The collection of cosets naturally forms a ring where

$$(a + I) + (b + I) := (a + b) + I \quad \text{and} \quad (a + I)(b + I) := ab + I.$$

This ring of cosets is called a *quotient ring* and is denoted R/I.

Remark 13. Think about general quotient rings in the same way you think about $\mathbb{Z}/nZ$. The ring R/I is just the ring R after setting all of the elements of I equal to 0. Another way to think about R/I is as a collection of equivalence classes: say $a, b \in R$ are equivalent if they differ by an element of I, i.e., $a = b + i$ of some element $i \in I$, i.e., $a - b \in I$. It is typical to denote the equivalence class of a by $\overline{a}$. We can then write $a = b \bmod I$ if $\overline{a} = \overline{b}$, i.e., if $a - b \in I$.

Definition 14. If I is an ideal of R, define the *(canonical) quotient mapping*

$$\begin{aligned} \pi\colon R &\to R/I \\ a &\mapsto \overline{a} = a + I. \end{aligned}$$

Exercise 15. Check that the quotient mapping $\pi\colon R \to R/I$ is a surjective homomorphism with kernel I.

Exercise 16. If $\phi\colon R \to S$ is a ring homomorphism, then $\mathrm{im}(\phi)$ is a ring with unity $\phi(1)$, and there is a well-defined isomorphism

$$\begin{aligned} \overline{\phi}\colon R/\ker(\phi) &\to \mathrm{im}(\phi) \\ a + \ker(\phi) &\mapsto \phi(a). \end{aligned}$$

Divisibility in rings

Definition 17. Let a, b be elements of a ring R. Then a divides b (in R) if there exists $c \in R$ such that $b = ac$. If a divides b, we write $a|b$.

Definition 18. Let R be a ring.

1. An element $u \in R$ is a *unit* if it has a multiplicative inverse. (In other words, there exists $v \in R$ such that $uv = 1$. Equivalently, $u|1$)
2. An element $p \in R$ is *prime* if is p not a unit, $p \neq 0$, and whenever $p|ab$, for some elements $a, b \in R$, then either $p|a$ or $p|b$.
3. An element $p \in R$ is *irreducible* if p is not a unit, $p \neq 0$, and whenever $p = ab$ for some elements $a, b \in R$, then either a or b is a unit.

Exercise 19. Let p be a prime in an integral domain. Then p is irreducible.

Example 20. The element $2 \in \mathbb{Z}$ is prime, but it factors into primes in $\mathbb{Z}[i]$ as $2 = (1+i)(1-i)$. Similarly, $x^2 + 1$ is prime in $\mathbb{R}[x]$ but factors into primes $x^2 + 1 = (x + i)(x - i) \in \mathbb{C}[x]$.

Proposition 21. Let R be a principal ideal domain, and let $r \in R$. Then r has a factorization

$$r = u \prod_{n=1}^{k} p_i^{e_i}$$

where u is a unit, the p_i are prime, each e_i is a positive integer, and $k \in \mathbb{N}$. The factorization is unique in the following sense; if $r = v \prod_{i=1}^{\ell} q_i^{f_i}$ for some unit v, primes q_i, positive integers f_i, and $\ell \in \mathbb{N}$, then $k = \ell$ and up to re-indexing, $p_i = u_i q_i$ with u_i a unit and $e_i = f_i$ for all i.

Proof. Math 332. □

Remark 22. A domain in which each element has a prime factorization as above is called a *unique factorization domain*, or UFD, for short. So the above proposition says that a PID is a UFD. To get a better sense of the meaning of unique factorization, consider the two factorizations into primes in $\mathbb{Z}$: we have $12 = 2 \cdot 3$ and $12 = -2 \cdot (-3)$. In the first factorization, the unit is 1 and the primes are 2 and 3. In the second factorization, the unit is -1 and the primes are 2 and -3. Note that $3 = (-1)(-3)$. So the primes 3 and -3 are the same up to multiplication by a unit.

Example 23. It turns out that if K is a field and $n > 1$, then $K[x_1, \ldots, x_n]$ is a UFD but not a PID. (For instance, in $\mathbb{R}[x, y]$, the ideal (x, y) cannot be generated by a single element.)

Proposition. In a principal ideal domain, an element is prime if and only if it is irreducible.

Proof. Math 332. □

Definition 24. Let R be a PID. A *greatest common divisor* of $a, b \in R$ is an element $d \in R$ such that

1. $d|a$ and $d|b$, and
2. if $e \in R$ with $e|a$ and $e|b$, then $e|d$.

We write $\gcd(a, b) = d$.

Proposition 25. Let R be a PID, and let $a, b \in R$. Then

1. There exists a greatest common divisor d of a, b.
2. $(a, b) = (d)$.
3. There exist $m, n \in R$ such that
$$ma + nb = d.$$
4. The greatest common divisors of a, b are exactly the elements of the form ud where u is a unit.

Proof. Since R is a PID, there exists $d \in R$ such that $(a, b) = (d)$. Since $a \in (d)$, There exists $c \in R$ such that $a = cd$. Thus, $d|a$. Similarly, $d|b$. Suppose e is an element of R such that $e|a$ and $e|b$. Since $d \in (a, b)$, there exist $m, n \in R$ such that $d = ma + nb$. Then, since $e|a$ and $e|b$, it follows that $e|d$. Thus, d is a greatest common divisor of a and b. We have proved all but the last part of the proposition.

Let e and d both be greatest common divisors of a and b. Then we have $e|d$ and $d|e$. So there exists $u, v \in R$ such that $e = ud$ and $d = ve$. It follows that

$$d = ve = vud.$$

Since R is an integral domain, the cancellation law holds. Therefore,

$$vu = 1.$$

So u is a unit.

Finally, it is straightforward to check that if d is a greatest common divisor of a and b, and u is a unit in R, then du is also a greatest common divisor of a and b. □

Corollary 26. Let R be a PID and suppose $a, b \in R$ have no prime factors in common. Then there exist $m, n \in R$ such that

$$ma + nb = 1.$$

Proof. Say the prime factorizations of a and b are

$$a = u\prod_{i=1}^{k} p_i^{e_i} \quad \text{and} \quad b = v\prod_{i=1}^{k} p_i^{f_i}.$$

Then the following is a greatest common divisor of a and b:

$$\gcd(a,b) = \prod_{i=1}^{k} p_i^{g_i}$$

where $g_i = \min\{e_i, f_i\}$ for each i. In particular, if a and b have no prime factors in common, $\gcd(a,b) = 1$, and the result follows from the preceding proposition. □

Proposition 27. Let R be a PID, and let $a \in R$. Then the ideal $I = (a)$ is maximal if and only if a is irreducible (and, hence, if and only if a is prime).

Proof. First suppose that I is maximal and assume that $a = bc$. It follows that $I = (a) \subseteq (b)$. Since I is maximal, there are two choices: either $(a) = (b)$ or $(b) = R$. If $(a) = (b)$, then there exists $d \in R$ such that $b = ad$. But then, $a = bc = adc$. Since R is an integral domain, we can cancel a to get $dc = 1$, which shows that c is a unit. If $(b) = R$, then since $1 \in R$, there exists $e \in R$ such that $eb = 1$, in which case, b is a unit. We have shown that if I is maximal, then a is irreducible.

For the converse, suppose that a is irreducible and that J is an ideal of R such that $J \supseteq I = (a)$. Since R is a PID, there exists $f \in R$ such that $J = (f)$. Then $J \supseteq I$ implies there exists $g \in R$ such that $a = fg$. Since a is irreducible, either f is a unit, in which case $J = R$, or g is a unit, in which case $J = I$. Hence, I is maximal. □

Division algorithm

Proposition 28. The ring $\mathbb{Z}$ is a principal ideal domain.

Proof. Let I be an ideal in $\mathbb{Z}$. If $I = (0)$, we are done. Otherwise, let a be the smallest positive element of I. Given any element $b \in I$, apply the division algorithm to find $q, r \in \mathbb{Z}$ such that

$$b = aq + r$$

with $0 \leq r < a$. Since $a, b \in I$, and I is an ideal,

$$r = b - aq \in I.$$

By the definition of a, it follows that $r = 0$. Hence, $b = aq$. We have shown that $I = (a)$. □

Let R be a ring. The *polynomial ring* $R[x]$ of polynomials in x with coefficients in R consists of elements of the form

$$f = \sum_{i=1}^{d} a_i x^i$$

for some $a_i \in R$ and some $d \in \mathbb{N}$. If $a_d \neq 0$, we say the *degree* of f is d, denoted $\deg(f) = d$. We assume the reader is familiar with addition and multiplication of polynomials. If R is a domain (for instance, if R is a field), then it is easy to check that

$$\deg(fg) = \deg(f) + \deg(g)$$

for any $f, g \in R[x]$. The ring R is a subset of $R[x]$. The elements of R are exactly the polynomials in $R[x]$ of degree 0.

Proposition 29. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Proof. Math 332. □

Proposition 30. Let K be a field. Then $K[x]$ is a principal ideal domain.

Proof. Let I be an ideal in $K[x]$. If $I = (0)$, we are done. Similarly, if I contains any nonzero element a of K, then a has a multiplicative inverse $b \in K$. By the definition of an ideal, since $a \in I$ and $b \in K \subset K[x]$, it follows that $ab = 1 \in I$. It then follows that $I = (1) = K[x]$. So again, I is principal. Now assume that $I \neq (0)$ and the only element of K contained in I is 0. So there exists an element f in I of smallest positive degree. Given $g \in I$, apply the division algorithm to find $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq r < \deg(f)$. Since I is and ideal and $f, g \in I$, it follows that

$$r = g - fq \in I.$$

By definition of f, it follows that $\deg(r) = 0$. Hence, $r \in K \cap I = \{0\}$, i.e., $r = 0$. It follows that $g = fq$. We have shown that $I = (f)$. □