Math 3030 Algebra I
Review of basic ring theory

1 Rings

Definition 1.1. *A* ***ring*** $(R, +, \cdot)$ *is a set* R *together with two binary operations:* ***addition*** *and* ***multiplication*** $+, \cdot : R \times R \to R$ *such that*

1. $(R, +)$ *is an abelian group;*
2. *(a)* $\cdot$ *is associative; and*
   (b) there exists a ***multiplicative identity*** *in* R*, i.e. an element* $1 \in R$ *such that* $a1 = 1a = a$ *for any* $a \in R$*.*
3. $\cdot$ *is distributive over* $+$*, i.e.*

$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc$$

for any $a, b, c \in R$*.*

Definition 1.2.
- *We say that a ring* R *is* ***commutative*** *if* $ab = ba$ *for any* $a, b \in R$*.*
- *A triple* $(R, +, \cdot)$ *satisfying all the above conditions except 2(b) is called a* **rng** *or a* **ring without identity**.

Here are some examples of rings:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (equipped with the usual addition and multiplication) are all commutative rings.
2. Let R be any commutative ring. Then the set of polynomials $R[x]$ with coefficients in R is also a commutative ring. Examples are $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.
3. For an integer $n \geq 2$, $n\mathbb{Z}$ is a commutative rng.
4. The only ring in which $1 = 0$ is $R = \{0\}$, called the **zero ring**. Any ring with $1 \neq 0$ is called a **nonzero ring**.
5. For any nonzero integer n, $\mathbb{Z}_n$ is a finite commutative ring.
6. Let R be any commutative ring. Then for any integer $n \geq 2$, the set $M_{n\times n}(R)$ of $n \times n$ matrices with entries in R is a noncommutative ring.

2 Special classes of rings

Definition 2.1. *Let R be a ring. If $a, b \in R$ are two nonzero elements of R such that $ab = 0$, then we call them **0-divisors**. (More precisely, a is called a **left 0-divisor** while b is called a **right 0-divisor**.)*

Definition 2.2. *An **integral domain** is a nonzero commutative ring which contains no 0-divisors.*

Proposition 2.3. *A nonzero commutative ring R is an integral domain if and only if the cancellation law hold for multiplication, i.e. whenever $ca = cb$ and $c \neq 0$, we have $a = b$.*

Examples:

1. The finite ring $\mathbb{Z}_n$ is an integral domain if and only if n is a prime.

2. If D is an integral domain, then the polynomial ring $D[x]$ is also an integral domain.

Definition 2.4. *Let R be a nonzero ring. A nonzero element $u \in R$ is called a **unit** if it has a multiplicative inverse in R, i.e. there exists $u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$.*

Definition 2.5. *A **field** is a nonzero commutative ring in which every nonzero element is a unit.*

It is not hard to see that any field is an integral domain. Conversely, we have the following

Proposition 2.6. *Any finite integral domain is a field.*

Examples:

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

2. By the above proposition, $\mathbb{Z}_p$ is a finite field for any prime p.

3. $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

Definition 2.7. *Let D be an integral domain. If there exists a positive integer n such that $na = 0$ for any $a \in D$, then D is said to be of **finite characteristic**, and the smallest such positive integer is called the **characteristic** of D, denoted by char(D). If no such integer exists, then we say D is of **characteristic 0**, written as char$(D) = 0$.*

Proposition 2.8. *If $n1 \neq 0$ for any positive integer n, then D is of characteristic 0. Otherwise, char$(D) =$* $\min\{n \in \mathbb{Z}_{>0} : n1 = 0\}$.

Proposition 2.9. *The characteristic of an integral domain is either 0 or a prime p.*

Examples:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0.

2. $\mathbb{Z}_p$ is of characteristic p.

Given an integral domain D, the **field of quotients** (or **fraction field**) of D, denoted by Frac(D), is the quotient of the product $D \times (D \setminus \{0\})$ by the equivalence relation:

$$(a, b) \sim (c, d) \text{ if and only if } ad = bc.$$

Proposition 2.10. *Frac(D) is a field under the addition and multiplication inherited from D, with additive identity $[(0,1)]$, multiplicative identity $[(1,1)]$, and the inverse of a nonzero element $[(a,b)]$ given by $[(b,a)]$.*

Furthermore, there is a natural embedding $j : D \hookrightarrow$ Frac(D) by $a \mapsto [(a,1)]$, which is universal *among all embeddings from D to a field, i.e. for any embedding $\iota : D \hookrightarrow L$ from D into a field L, there exists an embedding $i :$ Frac$(D) \hookrightarrow L$ such that $\iota = i \circ j$.*

Examples:

1. Frac$(\mathbb{Z}) = \mathbb{Q}$.
2. Let F be a field. Then Frac$(F[x])$ is called the **field of rational functions** over F, denoted by $F(x)$. Formally, we can write

$$F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x],\ g(x) \neq 0 \right\}.$$

3 Ring homomorphisms; subrings and ideals

Definition 3.1. *Let R and R' be rings. A map $\phi : R \to R'$ called a* ***ring homomorphism*** *(or simply* ***homomorphism****) if the following conditions are satisfied:*

1. *$\phi(1_R) = 1_{R'}$;*
2. *$\phi(a + b) = \phi(a) + \phi(b)$, for all $a, b \in R$;*
3. *$\phi(ab) = \phi(a)\phi(b)$, for all $a, b \in R$.*

If ϕ is furthermore bijective, then it is called an ***isomorphism****. We say that R is* ***isomorphic*** *to R', denoted by $R \cong R'$, if there exists an isomorphism ϕ from R to R'.*

Remark 3.2. *If ϕ is an isomorphism, then ϕ^{-1} is automatically an isomorphism.*

Examples of ring homomorphisms:

1. For any positive integer n, the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by mapping k to its reminder when divided by n is a surjective ring homomorphism.
2. Let R be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. Fix $a \in \mathbb{R}$. Then the **evaluation map** $\phi_a : R \to \mathbb{R}$ defined by $f \mapsto f(a)$ is a ring homomorphism.

Proposition 3.3. *A* ***subring*** *of a ring* $(R, +, \cdot)$ *is a subset* $S \subset R$ *containing* 1_R *and closed under* $+$ *and* $\cdot$ *which forms a ring under the inherited operations.*

Proposition 3.4. *Let* $\phi : R \to R'$ *be a ring homomorphism. Then*

- $\phi(0) = 0'$*, where* 0 *and* $0'$ *are the additive identities in* R *and* R' *respectively.*
- *For any* $a \in R$*,* $\phi(-a) = -\phi(a)$*.*
- *For any subring* $S \subset R$*,* $\phi(S)$ *is a subring of* R'*.*
- *For any subring* $S' \subset R'$*,* $\phi^{-1}(S')$ *is a subring of* R*.*

Remark 3.5. *Similar to groups, we can define the category* `Ring` *of rings. A free object on* n *generators in the category* `Comm Ring` *of commutative rings is given by the polynomial ring* $\mathbb{Z}[x_1, \ldots, x_n]$*. This places the polynomial ring on the same footing as the free group and finite dimensional vector spaces:*

$$\begin{aligned} F_{\mathtt{Grp}}(a_1, \ldots, a_n) &= \textit{free group on } n \textit{ generators}, \\ F_{\mathtt{Ab}}(a_1, \ldots, a_n) &= \mathbb{Z}^n, \\ F_{\mathtt{Vect}_F}(a_1, \ldots, a_n) &= F^n, \\ F_{\mathtt{Comm\ Ring}}(a_1, \ldots, a_n) &= \mathbb{Z}[x_1, \ldots, x_n]. \end{aligned}$$

Definition 3.6. *Let* $\phi : R \to R'$ *be a ring homomorphism. The additive subgroup*

$$\ker \phi := \phi^{-1}(0') = \{a \in R : \phi(a) = 0'\}$$

is called the ***kernel*** *of* ϕ*.*

Proposition 3.7. *A ring homomorphism* $\phi : R \to R'$ *is injective if and only if* $\ker \phi = \{0\}$.

Definition 3.8. *An additive subgroup* I *of a ring* R *such that* $aI \subset I$ *and* $Ib \subset I$ *for any* $a, b \in R$ *is called an* ***ideal*** *of* R*.*

Proposition 3.9. *For any homomorphism* $\phi : R \to R'$*,* $\ker \phi$ *is an ideal of* R*.*

Theorem 3.10. *Let* $I \subset R$ *be an additive subgroup. Then the multiplication*

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

on additive cosets is well-defined if and only if I *is an ideal.*

Corollary 3.11. *Let* $I \subset R$ *be an ideal. Then the additive cosets of* I *in* R *form a ring, called the* ***quotient ring*** *of* R *by* I *and denoted by* R/I*, under the operations*

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I, \\ (a + I)(b + I) &= (ab) + I. \end{aligned}$$

Proposition 3.12. *Let* $I \subset R$ *be an ideal. Then the map* $\pi : R \to R/I$ *defined by* $\pi(a) = a + I$ *is a surjective ring homomorphism with* $\ker \pi = I$*; this map is called the* ***projection map*** *or* ***canonical map****.*

Hence "ideal" and "kernel of a ring homomorphism" are *equivalent* concepts.

Theorem 3.13. *(First Isomorphism Theorem) Let $\varphi : R \to R'$ be a ring homomorphism. Let $I = \ker \varphi$. Then the map $\overline{\varphi} : R/I \to \varphi(R)$ defined by*

$$\overline{\varphi}(a + I) = \varphi(a)$$

is an isomorphism such that $\varphi = \overline{\varphi} \circ \pi$.

Here are some examples:

1. $n\mathbb{Z} \subset \mathbb{Z}$ is an ideal, and $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ as rings.

2. Let R be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. Fix $a \in \mathbb{R}$. Then $I_a := \{f \in R : f(a) = 0\}$ is an ideal of R since it is the kernel of the evaluation map ϕ_a, and $R/I_a \cong \mathbb{R}$ as rings. On the other hand, the subset S consisting of all constant functions is a subring but *not* an ideal.

3. For any ring R, both $\{0\}$ and R are ideals of R. An ideal $I \subsetneqq R$ is called **proper** and ideal $\{0\} \subsetneqq I \subset R$ is called **nontrivial**.

4. Let R be a commutative ring. Let $a \in R$. Then the set of all multiples of a

   $$\langle a \rangle := \{ra : r \in R\}$$

   is an ideal, called the **principal ideal generated by** a. Note that $R = \langle 1 \rangle$.

5. More generally, let $A \subset R$ be a nonempty subset of a commutative ring R. Then the set of all finite linear combinations of elements of A

   $$\langle A \rangle := \{r_1 a_1 + \cdots + r_k a_k : k \in \mathbb{Z}_{>0},\ r_i \in R,\ a_i \in A\}$$

   is an ideal, called the **ideal generated by** A.

Proposition 3.14. *Let F be a field.*

- *If char$(F) = 0$, then there exists an embedding $\mathbb{Q} \hookrightarrow F$.*
- *If char$(F) = p$, then there exists an embedding $\mathbb{Z}_p \hookrightarrow F$.*

Because of this, the fields $\mathbb{Q}$, $\mathbb{Z}_p$ (where p is a prime) are called ***prime fields****.*

4 Polynomial rings

Definition 4.1. *Let R be a nonzero commutative ring. A* ***polynomial*** *$f(x)$ with coefficients in R is a formal sum*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

where $a_i \in R$ and $a_i = 0$ for all but finitely many i's. If $a_i \neq 0$ for some i, then the largest such integer is called the ***degree*** *of $f(x)$. We denote by $R[x]$ the set of all polynomials with coefficients in R.*

Proposition 4.2. *$R[x]$ is a commutative ring under the usual addition and multiplication of polynomials.*

Proposition 4.3 (Division algorithm)**.** *Let F be a field. Let $f(x), g(x) \in F[x]$ be two nonzero polynomials. Then there exist unique $q(x), r(x) \in F[x]$ such that*

$$f(x) = q(x)g(x) + r(x),$$

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Corollary 4.4. *An element $a \in F$ is a **root** (or **zero**) of $f(x)$ (i.e. $f(a) = 0$) if and only if $f(x)$ is divisible by $x - a$.*

Corollary 4.5. *A nonzero polynomial $f(x) \in F[x]$ of positive degree n can have at most n roots in F.*

Definition 4.6. *An integral domain D is called a **principal ideal domain (PID)** if every ideal in D is principal.*

An example of PID is given by $\mathbb{Z}$.

Proposition 4.7. *For any field F, $F[x]$ is a PID.*

Definition 4.8. *A nonconstant polynomial $f(x) \in F[x]$ is said to be **irreducible over** F if it cannot be written as a product $g(x)h(x)$ where both $g(x)$ and $h(x)$ have degrees lower than that of $f(x)$. Otherwise, $f(x)$ is said to be reducible.*

Examples:

1. $x^2 + 1$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.
2. $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$ since it has no roots in $\mathbb{Z}_5$ (which is easy to check).

Lemma 4.9 (Gauss' lemma)**.** *If $f(x) \in \mathbb{Z}[x]$ can be factored as a product of two polynomials in $\mathbb{Q}[x]$, it can also be factored as a product of two polynomials in $\mathbb{Z}[x]$.*

Theorem 4.10 (Eisenstein criterion)**.** *Let $p \in \mathbb{Z}$ be a prime. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Suppose that $p \nmid a_n$, $p : a_i$ for all $i < n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Examples:

1. $5x^5 - 9x^4 - 3x^2 - 12$ is irreducible over $\mathbb{Q}$.
2. For any prime p, the **p-th cyclotomic polynomial**

   $$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

   is irreducible over $\mathbb{Q}$.

Theorem 4.11. *Let F be a field. For any polynomial $f(x) \in F[x]$, the following statements are equivalent:*

1. *$F[x]/\langle f(x) \rangle$ is a field.*
2. *$F[x]/\langle f(x) \rangle$ is an integral domain.*
3. *$f(x)$ is irreducible over F.*