MATH 593 - Ring

ARessegetes Stery

September 30, 2023

Contents

1 Ring homomorphism, Quotient Ring

Definition 1.1 (Ring Homomorphism). *Let X, Y be rings. A **Ring Homomorphism** is a map $f : X \to Y$ satisfying the following properties:*

- $f(1) = 1$.
- $\forall x_1, x_2 \in X, f(x_1) + f(x_2) = f(x_1 + x_2)$.
- $\forall x_1, x_2 \in X, f(x_1 x_2) = f(x_1) f(x_2)$

Definition 1.2 (Quotient Ring). *Let R be a ring and $I \subseteq R$ a two-sided ideal. The **Quotient Ring** (R/I) is defined as $(R/\sim)$ with an equivalence relation $\sim$ where $a \sim b$ if and only if $a - b = I$. Elements in (R/I) are denoted as $\bar{a}$, where $\bar{a} = \bar{b}$ if and only if $a \sim b$.*

The natural homomorphism $\pi_I : R \to (R/I)$ is defined as $\pi(a) = \bar{a}$, which satisfies the *universal property of quotient rings*:

Theorem 1.1 (Fundamental Theorem of Ring Homomorphisms). *Let $\varphi : R \to S$ be a ring homomorphism, I a two-sided ideal s.t. $I \subseteq \ker \varphi$, and π be the natural ring homomorphism from R to (R/I). Then there exists a unique ring homomorphism $f : R/I \to S$ s.t. the following diagram commutes, i.e. $\varphi = f \circ \pi$.*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & S \\ & R/I \arrow[u, "f"'] \end{tikzcd}$$

Proof. It suffices to prove that f exists and is unique, and verify that f is indeed a ring homomorphism.

- **Uniqueness.** By the requirement that f should make the diagram commute, $f(\bar{a}) = \varphi(a),\ \forall a \in R$. Uniqueness of f follows from the fact that φ maps every element in R to a unique element in S.
- **Existence.** It suffices to verify that f is well-defined, i.e. does not vary w.r.t. change of representative in (R/I). For all $a, b \in R$ s.t. $\bar{a} = \bar{b}$, $(a - b) \in I \implies \varphi(a - b) = 0 \implies \varphi(a) = \varphi(b)$ since φ is a ring homomorphism. By the uniqueness of f it is specified that $f(\bar{a}) = \varphi(a)$, which implies that for all $\bar{a} = \bar{b} \in (R/I)$, $f(\bar{a}) = \varphi(a) = \varphi(b) = f(\bar{b})$.
- f **is indeed a homomorphism.** This follows from the fact that φ is a ring homomorphism.

$\square$

2 Ring of Fractions

Definition 2.1 (Multiplicative System). *A subset $S \subseteq R$ for a ring R is a **multiplicative system** if $1 \in S$, and $\forall s_1, s_2 \in S, s_1 \cdot s_2 \in S$, where $\cdot$ is the multiplication in R.*

Definition 2.2 (Ring of Fractions). *Let R be a commutative ring, with $S \subseteq R$ a multiplicative subset, the **ring of fraction** $S^{-1}R$ is defined as $R \times S/\sim$, where $(s_1, r_1) \sim (s_2, r_2)$ if and only if there exists $t \in R$ s.t. $t(s_1 r_2 - s_2 r_1) = 0$. $(s, r) \in S^{-1}R$ is denoted as $\frac{s}{r}$. The definition of operations follows directly from analogy of that in $\mathbb{Q}$.*

The natural homomorphism (inclusion map) from R to $S^{-1}R$ is defined as $r \hookrightarrow \frac{r}{1}$.

Remark 2.1. If R is an integral domain, then $(s_1, r_1) \sim (s_2, r_2)$ iff $s_1 r_2 = s_2 r_1$, as for $\mathbb{Q}$.

Remark 2.2. *If R is not an integral domain, and S contains zero divisors, then the inclusion map ceases to be injective, as choosing t s.t. it satisfies $ts_1 = ts_2 = 0$ for some s_1, s_2 that are zero divisors gives $\varphi(s_1) = \varphi(s_2)$. Changing R to an integral domain guarantees that the inclusion map φ is injective.*

Proposition 2.1. *$\sim$ is an equivalence relation.*

Proof. It is clear that $\sim$ is reflexive and symmetric. For transitivity, consider $(s_1, r_1) \sim (s_2, r_2) \wedge (s_2, r_2) \sim (s_3, r_3)$. That is, there exists some $t_1, t_2 \in R$ s.t.

$$\begin{cases} t_1(s_1 r_2 - s_2 r_1) = 0 \\ t_2(s_2 r_3 - s_3 r_2) = 0 \end{cases} \implies t_1 t_2 (s_1 r_2 s_3 - s_2 r_1 s_3) = t_1 t_2 (s_1 s_2 r_3 - s_2 r_1 s_3) = t_1 t_2 s_2 (s_1 r_3 - s_3 r_1) = 0$$

□

Remark 2.3. *Notice that if $s \in S$, then $\frac{s}{a}$ for $a \in R$ is invertible. This tends more to a field, with more elements being "reachable" via multiplying an element from one side. A direct consequence is that less ideals exist in $S^{-1}R$, with ideals in R whose generators differ by a factor that divides s being identified in $S^{-1}R$.*

Remark 2.4. *It is required that R is commutative is to preserve the most structures from R, i.e. ensure that $S^{-1}I$ is an ideal for all ideals in R. This is due to the addition in action:*

$$\forall \frac{r_1}{s_1}, \frac{r_2}{s_2} \in S^{-1}R, \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2}$$

which indicates that $S^{-1}I$ is a two-sided ideal if and only if $I \subseteq R$ is a two-sided ideal. For one-sided (left/right) ideal the property is not fully inherited.

Theorem 2.1 (Universal Property of Ring of Fractions). *Suppose R and T are commutative rings, with φ the inclusion of R into $S^{-1}R$. Then for $f : R \to T$ s.t. $\forall s \in S, f(s)$ is invertible in T, there exists a unique ring homomorphism g s.t. $f = g \circ \varphi$, i.e. make the following diagram commute:*

Proof. Adopt the same strategy as in the previous section:

- **Existence.** For all $\frac{a}{s} \in S^{-1}R$, $g(\frac{a}{s}) := f(a)(f(s))^{-1}$ which is well-defined since f is required to map all elements in S to invertible elements. g being a ring homomorphism follows from the fact that f is a ring homomorphism.

$$\begin{tikzcd} R \arrow[r, hook, "\varphi"] \arrow[dr, "f"'] & S^{-1}R \arrow[d, "g"] \\ & T \end{tikzcd}$$

- **Uniqueness.** Follows from specifying $g(\frac{a}{s}) := f(a)(f(s))^{-1}$.

□

Remark 2.5. *If $S := R \setminus \{0\}$, then $S^{-1}R$ is the whole field, with localization equivalent to completion of inverse of R.*

2.1 Localization of a Ring

Definition 2.3. *A commutative ring $R \neq \{0\}$ is **local** if it admits a unique maximal ideal M. Local rings are denoted by a pair (R, M).*

Example 2.1. Let R be a commutative ring, with $\mathfrak{p} \subseteq R$ a prime ideal. Let $S = R \setminus p$ be a multiplicative system. Then the ring $S^{-1}R$ is local, with the maximal ideal of it being $S^{-1}\mathfrak{p}$. This results from the fact that $S^{-1}I$ is an ideal if and only if I is an ideal in R. Further since $\mathbb{Z}$ is a PID (see next section), all prime ideals are maximal, $S^{-1}\mathfrak{p}$ is indeed maximal. The fact that there is only one such maximal ideal results from that all other primes are in S, i.e. $S^{-1}\mathfrak{p}' = S^{-1}R$ for all $\mathfrak{p}' \neq \mathfrak{p}$.

Proposition 2.2. *Let $R \neq \{0\}$ be a commutative ring. Then R being local if and only if for all $a \in R$, either a is invertible or $(1-a)$ is invertible. In this case, the maximal ideal M is the set of all non-invertible elements.*

Proof. Proceed by showing implication in both directions:

$\Rightarrow$: Suppose that (R, M) is the local ring of interest. Proceed by showing a contradiction: suppose that both a and $(1-a)$ are non-invertible. Then since R is local $(a) \subseteq M$, $(1-a) \subseteq M$ indicating that $1 \in M$ which is a contradiction. In this case for all a non-invertible, $(a) \subseteq M$, which implies that M is the set of all non-invertible elements.

$\Leftarrow$: Define set $M := \{a \in R \mid \forall x \in R, ax \neq 1\}$. By construction if M is an ideal then it must be maximal, as including an invertible element expands the ideal to the whole ring. Verify that M is indeed an ideal:

- *Closed with addition.* Proceed via showing that the contraposition. Suppose that there exists $a, b \in R$ s.t. both a and b are non-invertible, but there exists some $c \in R$ s.t. $c(a+b) = 1$. Then $ca = 1 - (cb)$ is non-invertible, which implies that $1 - ca$ is invertible. But notice $1 - ca = cb$ is also non-invertible, which is a contradiction.
- *Absorption with multiplication.* This simply results from the fact that a non-invertible element multiplied by a unit is still non-invertible.

□

3 Polynomial Rings

Definition 3.1 (R-algebra)**.** *Let R be a ring. Then a ring S is an R-**algebra** for the specific R mentioned if there exists a ring homomorphism $\varphi : R \to S$ s.t. $\forall r \in R, s \in S, \varphi(r)s = s\varphi(r)$. When the homomorphism needs to be specified, the algebra is often denoted as a pair $\langle S, \varphi\rangle$*

Remark 3.1. *An R-algebra is a two-sided R-module, which can be regarded as a generalization of the structure in R. R itself is not necessarily commutative, which implies that the associated homomorphism maps R to the center of S.*

Definition 3.2 (Morphism of R-algebras)**.** *Let $\langle R_1, f_1\rangle, \langle R_2, f_2\rangle$ be R-algebras. A **Morphism of R-algebras** is a ring homomorphism $\varphi : R_1 \to R_2$ s.t. the following diagram commute; i.e. $f_2 = \varphi \circ f_1$:*

$$\begin{tikzcd} R \arrow[r, "f_1"] \arrow[dr, "f_2"] & R_1 \arrow[d, "\varphi"] \\ & R_2 \end{tikzcd}$$

Definition 3.3 (R-subalgebra)**.** *Let $\langle S, f_s\rangle$ be a R-algebra for R a ring. $\langle T, f_t\rangle$ is a R-**subalgebra** of S if T is a R-algebra, with $f_t(R) \subseteq S$; and there exists a morphism φ from T to S, i.e. φ makes the following diagram commute:*

$$\begin{tikzcd} R \arrow[r, "f_t"] \arrow[dr, "f_s"] & T \arrow[d, hook, "\varphi"] \\ & S \end{tikzcd}$$

Definition 3.4 (Polynomial Ring)**.** *Let R be a commutative ring. The **polynomial ring of** R, denoted $R[x]$, is defined as*

$$R[x] := \left\{ \sum_{i=0}^{n} c_i x^i \mid n \in \mathbb{N}, c_i \in R \right\}$$

with the addition and multiplication the same as in polynomials over $\mathbb{Z}$. The natural inclusion from R to $R[x]$ is defined as $r \mapsto r$ which is a polynomial of degree 0.

Remark 3.2. *If R is a domain, then $R[x]$ is also a domain (consider the product of terms with highest degree); where $\deg(fg) \leq \deg(f) + \deg(g)$.*

Theorem 3.1 (Universal Property of Polynomial Ring)**.** *Let R be a ring and $\langle S, f\rangle$ an R-algebra, and φ be the inclusion map from R to $R[x]$. For all $s \in S$, there exists a unique morphism of R-algebra $g : R[x] \to S$ s.t. $g(x) = a$, and the following diagram commutes, i.e. $f = g \circ \varphi$:*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, hook, "f"] & R[x] \arrow[d, "g"] \\ & S \end{tikzcd}$$

Proof. Proceed similarly by first determining the form that g takes, and then showing the uniqueness and existence.

- **Uniqueness.** Since it is required that g is a morphism of R-algebras, we have

$$g\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} g(a_i)g(x^i) = \sum_{i=0}^{n} f(a_i)g(x^i) = \sum_{i=0}^{n} f(a_i)a^i$$

  by the requirement that $g(x) = a$. This is the only form that g could take, and thus proves its uniqueness.

- **Existence.** For existence it suffices to check that g is indeed a ring homomorphism. By the uniqueness g is fixed by sending $x \in R[x]$ to $a \in R$. Notice that R is commutative, which indicates that both left and right composition is satisfied; with the addition condition verified in the uniqueness part.

$\square$

Theorem 3.2 (Universal Property of Polynomial Ring of Several Variables)**.** *Let A be a commutative R-algebra and g be the inclusion map from R to $R[x_1, \cdots, x_n]$ with a fixed n. For every R-algebra S and $(a_1, \cdots, a_n) \in S$, there exists a unique homomorphism of R-algebra $h : R[x_1, \cdots, x_n] \to S$ s.t. $h(x_i) = a_i$ for all $i \in [\![1, n]\!]$, and the following diagram commutes, i.e. $f = h \circ g$:*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, hook, "g"'] & S \\ & R[x_1, \cdots, x_n] \arrow[u, "h"'] \end{tikzcd}$$

Sketch of Proof. The idea is similarly consider substitution $x_i \mapsto a_i$, and proceed to verify that this is indeed a ring homomorphism. One step that requires caution is that polynomials of several variables are defined in an inductive manner; therefore here proof should also be done inductively, on the number of variables involved. $\square$

Using polynomial of several variables, it is clearer to formalize the "generating set" of a ring via specifying which element each variable maps to:

Definition 3.5 (Finitely Generated R-algebra)**.** *Let R be a commutative ring, with A a commutative R-algebra. Fix $(a_1, \cdots, a_n) \in A$. By the universal property of polynomial of several variables, there exists a unique homomorphism $\varphi : R[x_1, \cdots, x_n]$ s.t. $\varphi(x_i) = a_i$. Then the subalgebra* $\operatorname{im}\varphi$ *is said to be **generated** by $\{a_1, \cdots, a_n\}$.*

Remark 3.3. *Using the same formalization as in the definition above,* $\operatorname{im}\varphi$ *is smallest R-subalgebra of A that contains $\{a_1, \cdots, a_n\}$.*

Proof. It is clear that $\operatorname{im}\varphi$ contains $\{a_1, \cdots, a_n\}$. To see that it is smallest, suppose there is a smaller one A', then there must be some $\sum_{i=0}^{n} a_i x^i \notin A'$, which contradicts with the fact that a ring should be closed. $\square$

Notice that in the definition of polynomial ring it is only required that x could be multiplied with powers of itself. This enables making polynomial a representation of groups:

Definition 3.6 (Group Ring). *Let R a commutative ring, and G a group. A* ***group ring of*** *R* ***on*** *G is defined as*

$$R[G] := \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}$$

with the addition and multiplication the same as that in the polynomial ring.

Remark 3.4. *The operation between the ring and the group is not required to be defined and is simply a notation. The polynomial cannot admit any structure that is more complicated (e.g. changing the group to be a ring) as otherwise the addition will not be well-defined.*

4 Ideals

Definition 4.1 (Finitely-Generated Ideals). *Let R be a ring. Then*

- *Let (I_α) be a family of ideals for $\alpha \in \Lambda$ the index set, then the* ***ideal generated by (sum of)*** *(I_α) is defined as*

$$\sum_{\alpha \in \Lambda' \subseteq \Lambda} I_\alpha := \left\{ \sum_{\alpha \in \Lambda'} a_\alpha \middle| a_\alpha \in I_\alpha, |\Lambda'| \text{ finite} \right\}$$

- *Alternatively one could consider the* ***ideal generated by (product of)*** *two ideals (which can be easily extended to several ideal cases) I and J to be*

$$I \cdot J := \left\{ \sum_{i=1}^{n} a_i b_i \middle| n \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \forall i \right\}$$

- *Suppose further that R is commutative. Let $\Lambda := \{\lambda_1, \cdots, \lambda_n\}$ be a subset of R. Then the* ***ideal generated by*** *Λ is defined as*

$$(\lambda_1, \cdots, \lambda_n) := \left\{ \sum_{k=1}^{n} r_k \lambda_k \middle| r_k \in R \right\}$$

Remark 4.1. *Ideals generated by only one element is principal. For finitely generated ideals, the ideal generated by a set of elements is the same as the ideal generated by the corresponding principal ideals of the elements. This simply results from the fact that $(a) = \{ra | r \in R\}$.*

Specify R to be a commutative ring, with $I \subseteq R$ an ideal of R. Consider the following special cases of ideals:

Definition 4.2 (Radical Ideal). *$I \subseteq R$ is a* ***radical ideal*** *if for all $a \in R$, $\exists n \in \mathbb{Z}_{>0}\ a^n \in I \implies a \in I$.*

Definition 4.3 (Prime Ideal). *$I \subseteq R$ is a* ***prime ideal*** *if $I \neq R$, and for all $a, b \in R$, $ab \in I \implies (a \in I) \vee (b \in I)$.*

Definition 4.4 (Maximal Ideal). *$I \subseteq R$ is a* ***maximal ideal*** *if $I \neq R$; and there is no ideal J in R s.t. $I \subsetneq J \subsetneq R$.*

Remark 4.2. *Recall that R is a domain if and only if for all $a, b \in R$, $ab = 0 \implies a = 0 \vee b = 0$. This implies that for any ring R with $\mathfrak{p}$ a prime ideal in it, $R/\mathfrak{p}$ is a domain.*

Definition 4.5 (Reduced Ring). *A R is a* ***reduced ring*** *if and only if it does not have any nilpotent elements, i.e. for all $u \in R$, $u^n = 0 \implies u = 0$ for all $n \in \mathbb{Z}_{>0}$.*

Remark 4.3. *For a commutative ring R, I is a radical ideal if and only if R/I is a reduced ring.*

Proposition 4.1. *I is a maximal ideal if and only if R/I is a field.*

Proof. This fact follows directly from the following simple lemma. □

Lemma 4.1. *$R = K$ is a field if and only if it only has two ideals (0) and (1).*

Proof. Consider in both directions:

- ⇒: If K is a field, then either there are no invertible elements, which in this case the ideal I can only contain 0 as this is the only non-invertible element in a field; or 1 and therefore every element is in the ideal, as $\forall g \in I, \exists g^{-1} \in K, gg^{-1} = 1 \in I$.
- ⇐: If a ring R has only two ideals (0) and (1), then for all $0 \neq u \in R$ consider (u). By hypothesis $(u) = (1)$, i.e. there exists some $u^{-1} \in R$, which implies that R is actually a field.

□

Proposition 4.2. *An ideal being maximal implies that it is prime; and an ideal being prime implies that it is radical.*

Proof. Maximal ideals are prime. Suppose that $I \subseteq R$ is maximal but is not prime, i.e. there exists some $a, b \in R$ s.t. $ab \in R, a \notin R, b \notin R$. By hypothesis $I \cup \{a\} = R.$, i.e. there exists some $r \in R, t \in I$ s.t. $a + rt = 1$. But then $b = ba + (br)t \in I$ which is a contradiction.

Prime ideals are radical. Consider inductively on a and a^{n-1}; apply the definition of prime ideals. □

Example 4.1. Consider counterexamples of the converse of the proposition above:

- $\mathbb{Z}_N$ for N not a power of prime is radical, but not prime.
- A trivial case for an ideal being prime but not maximal is (0), where as long as the ring is not a field, it is maximal.
- A more interesting case for an ideal being prime but not maximal is for finitely generated non-PIDs, adding a generator to a prime ideal suffices to create a "larger" ideal. Take the example $(x) \subseteq R[x]$ where R is a domain, which is prime as $R[x]/\langle x\rangle \cong R$ is also a field. But $(x) \subseteq (2, x)$ which is not the whole ring.

5 Noetherian Ring

6 Euclidean Domain, PIDs and UFDs