Algebra III

Kexing Ying

July 24, 2021

N.B. this course has large overlap with the second year course *Groups and Rings* in particular, the ring subsection. Thus, most revisited proofs are simply omitted or replaced with a hint.

Contents

1 Fundamental Definitions

We will in this section recall some fundamental definitions which we will study throughout the course.

Definition 1.1 (Ring)**.** A ring R is a set together with two distinct elements $0_R, 1_R$, and two binary operations $+_R, \times_R : R^2 \to R$ such that

- $(R, +_R)$ is an additive abelian group with identity 0_R;
- $(R, \times_R)$ is a multiplicative abelian monoid with identity 1_R;
- $\times_R$ distributes over $+_R$, i.e. for all $r, s, t \in R$,

  $$(r +_R s) \times_R t = r \times_R t +_R s \times_R t,$$

  and

  $$r \times_R (s +_R t) = r \times_R s +_R r \times_R t.$$

We note that there is some ambiguity in the literature in the definition of a ring, and in particular, some might call the definition above as a commutative unital ring. We will in this course mostly consider ourselves with this definition, though we might later consider non-commutative rings.

Definition 1.2 (Field)**.** A field F is a ring is for all $f \in F \ \{0_F\}$, there exists some $f^{-1} \in F$ such that $f \times_F f^{-1} = 1_F$.

We will simply drop the subscript from the operations and the elements from these definitions whenever there is no confusion.

Recall that one method of constructing a ring from another is the polynomial ring. Let R be ring, then a polynomial on X is a sum

$$\sum_{n=0}^{\infty} a_n X^n$$

for some $(a_n)_{n \in \mathbb{N}} \subseteq R$ where all but finitely many a_i are zero. We say $P(X) = \sum_{n=0}^{\infty} a_n X^n$ has degree d if d is the largest number such that $a_d \neq 0$.

Definition 1.3 (Polynomial Ring)**.** Given a ring R, the polynomial ring $R[X]$ is the set of polynomials equipped with the operations $+_{R[X]}$ and $\times_{R[X]}$ such that

$$\sum_{n=0}^{\infty} a_n X^n +_{R[X]} \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n + b_n) X^n,$$

and,

$$\sum_{n=0}^{\infty} a_n X^n \times_{R[X]} \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) X^n.$$

It is not difficult to see that the ring axioms are satisfied and in fact, it is possible to construct polynomial rings with infinite degrees, though this shall not be considered in this course. An equivalent way of considering elements of polynomial rings is to see them as sequences with finite non-zero elements.

One may adjoin a polynomial ring with another variable, that is $R[X][Y]$ and by writing out the elements, we see that $R[X][Y] \cong R[Y][X]$ and we may instead write $R[X, Y]$ with no ambiguity.

1.1 Subrings and Extensions

Definition 1.4 (Subring)**.** A subring of the ring R is a subset of R containing $0, 1$ and is closed under $+$ and $\times$.

It is clear that a subring of a ring is a ring itself with the inherited operations.

Proposition 1.1. If S, T are subrings of the ring R, then so is $S \cap T$.

Definition 1.5. Given a subring S of R, $S[\alpha]$ for some $\alpha \in R$ is the subset of R consisting of all elements of R that can be expressed as $r_0 + r_1\alpha + \cdots + r_n\alpha^n$ for $r_i \in S$ and $n \in \mathbb{N}$. We call this process the adjoining of S with α.

Clearly $S[\alpha]$ contains 0 and 1 (as $S \subseteq S[\alpha]$) and is closed under $+$ and $\times$, and thus, is a subring of R.

An important example of the above construction is the following. Consider $\mathbb{Z} \subseteq \mathbb{C}$, we have $\mathbb{Z}[i]$ constructed through the definition above is known as the Gaussian integers is a subring of $\mathbb{C}$ consisting of all elements of the form $a+bi$ for $a, b \in \mathbb{Z}$. To see this, consider if $X^2 - rX - s$ is a polynomial of integer coefficients with complex root $\alpha \notin \mathbb{Z}$, then, we may consider $\mathbb{Z}[\alpha]$. As $\alpha^2 - r\alpha - s = 0$, we obtain $\alpha^2 = r\alpha + s$ and thus, for all $r_0 + r_1\alpha + \cdots + r_n\alpha^n \in \mathbb{Z}[\alpha]$,

$$\begin{aligned} r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_n\alpha^n &= r_0 + r_1\alpha + r_2(r\alpha + s) + \cdots \\ &= (r_0 + r_2 s + \cdots) + (r_1 + r_2 r + \cdots)\alpha. \end{aligned}$$

Hence, all elements of $\mathbb{Z}[\alpha]$ are of the form $a + b\alpha$ for $a, b \in \mathbb{Z}$.

On the other hand, if we consider $\mathbb{Z}[\pi] \subseteq \mathbb{C}$, as π is not an algebraic number, for all $P(X) \in \mathbb{Z}[X] \quad \{0\}$, $P(\pi) \neq 0$. Thus, if $P(X), Q(X)$ are polynomials such that $P(\pi) = r_0 + r_1\pi + \cdots + r_n\pi^n = s_0 + s_1\pi + \cdots + s_m\pi^m = Q(\pi)$, WLOG. $n \leq m$ we have $0 = (s_0 - r_0) + (s_1 - r_1)\pi + \cdots + (s_n - r_n)\pi^n + s_{n+1}\pi^{n+1} + \cdots + s_m\pi^{m+1}$, implying $s_i = r_i$ for all $i = 1, \cdots, n$ and $s_i = 0$ for $i > n$, we have $P = Q$. Hence, $\mathbb{Z}[\pi] \cong \mathbb{Z}[X]$.

Proposition 1.2. If R is a subring of S, then $R[\alpha]$ for some $\alpha \in S$ is the intersection of all subrings of S containing $R \cup \{\alpha\}$.

Proof. Since $R[\alpha]$ contains both R and α, we have

$$\bigcap \{U \mid R \cup \{\alpha\} \subseteq U \leq S\} \subseteq R[\alpha].$$

On the other hand, for all subrings U containing $R \cup \{\alpha\}$, $R[\alpha] \subseteq U$ as U is closed under $+$ and $\times$. Thus,

$$\bigcap \{U \mid R \cup \{\alpha\} \subseteq U \leq S\} = R[\alpha].$$

□

Definition 1.6 (Integral Domain)**.** A ring R is an integral domain if for all $r, s \in R$, $rs = 0$ implies $r = 0$ or $s = 0$.

In particular, we say $r \in R$ is a zero divisor if there exists a $s \in R \setminus \{0\}$ such that $rs = 0$. Thus, an integral domain is simply a ring with no zero divisors.

Definition 1.7 (Field of Fractions)**.** For R an integral domain, then the field of fractions of R denoted $\mathrm{Frac}(R)$, is $R \times R \setminus \{0\}$ quotiented by the equivalence class

$$(a, b) \sim (r, s) \iff as = br.$$

We write a/b as a representative of the equivalence class $[a, b]$.

We may equip the field of fractions of R with addition and multiplication such that for $a/b, r/s \in \mathrm{Frac}(R)$

$$\frac{a}{b} + \frac{r}{s} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \times \frac{r}{s} = \frac{ar}{bs}.$$

It is routine to check these operations are well-defined and that the ring axioms are satisfied. Furthermore, as the name suggests, $\mathrm{Frac}(R)$ is a field and for all $a/b \neq 0$, $(a/b) \times (b/a) = 1$.

Definition 1.8 (Multiplicative System)**.** A set $S \subseteq R$ is a multiplicative system if $1 \in S, 0 \notin S$ and is closed under multiplication.

Definition 1.9. Let R be a ring and $S \subseteq R$ be a multiplicative system. Then $S^{-1}R$ is $R \times S$ quotiented by the equivalence class

$$(a, b) \sim (r, s) \iff as = br$$

for $a, r \in R, b, s \in S$.

Similarly, we may equip $S^{-1}R$ with addition and multiplication such that $S^{-1}R$ is a subring of $\mathrm{Frac}(R)$.

It is possible to use this construction on rings which are not integral domains, though in that case, the equivalence class is more subtle as division by a zero divisor will introduces other elements into the subring. This will be explored later in this course.

1.2 Homomorphisms and Ideals

We recall the definition of ring homomorphism and some related results (whose proofs omitted or shortened).

Definition 1.10 (Ring Homomorphism)**.** Given R, S rings, a ring homomorphism from R to S is a map $f : R \to S$ such that for all $a, b \in R$,

- $f(1_R) = 1_S$;
- $f(a +_R b) = f(a) +_S f(b)$;
- $f(a \cdot_R b) = f(a) \cdot_S f(b)$.

If f is a bijection then we say f is an isomorphism.

Automatically, it is not difficult to see that condition 2 implies $f(0_R) = 0_S$ and from this we can deduece properties such as $f(-x) = -f(x)$.

Proposition 1.3. The image of a ring homomorphism $f : R \to S$ is a subring of S.

As we have seen in other contexts, the notion of an isomorphism is often defined to be a invertible structure preserving map. Though in some contexts, such as topological spaces, bijection is often not enough and we will require the inverse to be structure preserving. The following proposition shows that these two cases are equivalent for rings.

Proposition 1.4. If $f : R \to S$ is an isomorphism, then $f^{-1} : S \to R$ is a ring homomorphism.

Proof. For all $a, b \in S$, we have $f^{-1}(a+b) = f^{-1}(f(f^{-1}(a)) + f(f^{-1}(b))) = f^{-1}(f(f^{-1}(a) + f^{-1}(b))) = f^{-1}(a) + f^{-1}(b)$. Similar argument for the other conditions. $\square$

Proposition 1.5. There exist a unique homomorphism from $\mathbb{Z}$ to R for all ring R.

Proof. Clear by considering if $f : \mathbb{Z} \to R$ is a homomorphism, $f(n_{\mathbb{Z}}) = n_{\mathbb{Z}} \cdot 1_R$. $\square$

Proposition 1.6. Given a ring R and $\alpha \in R$, there exists a unique homomorphism $f : R[X] \to R$ such that $f(X) = \alpha$ and $f\mid_R = \mathrm{id}_R$. This homomorphism is called the evaluation map at α and we denote it as ev_α.

Proof. Clear and as the name suggests, the unique map is

$$\mathrm{ev}_\alpha(P(X)) = P(\alpha),$$

for all $P \in R[X]$. $\square$

More generally, if $f : R \to S$ is a homomorphism and $\alpha \in S$, there exists a unique $\mathrm{ev}_{f,\alpha} : R[X] \to S$ such that $\mathrm{ev}_{f,\alpha}\mid_R = f$ and $\mathrm{ev}_{f,\alpha}(X) = \alpha$. Furthermore, if f is simply the inclusion map from $R \to S$, image of $\mathrm{ev}_{f,\alpha}(X) = \alpha$ is $R[\alpha]$.

Definition 1.11 (Kernel)**.** Let R, S be rings and $f : R \to S$ a ring homomorphism. Then the kernel of f is

$$\ker f := \{r \in R \mid f(r) = 0_S\}.$$

Proposition 1.7. A ring homomorphism $f : R \to S$ is injective if and only if $\ker f = \{0\}$.

Definition 1.12 (Ideal)**.** Given a subset I of a ring R, then I is said to be an ideal if

- $0_R \in I$;
- for all $a, b \in I$ then $a + b \in I$;
- for all $a \in I$, $r \in R$, $ra \in I$.

Definition 1.13. The following ideals are important enough to warrant a definition.

- $\{0_R\} \subseteq R$ is the zero ideal;
- $R \subset R$ is the unit idea;
- for all $r \in R$, $\langle r \rangle := \{rs \mid s \in R\}$ is the principal ideal generated by r.

Proposition 1.8. Every ideal of $\mathbb{Z}$ is principle.

Proposition 1.9. In intersection of ideals is an ideal. Similarly, the sum of two ideals, i.e. if I, J are ideals, then $\{i + j \mid i \in I, j \in J\}$ is an ideal.

Definition 1.14. Let R be a ring and $r_1, \cdots, r_n \in R$. Then the ideal generated by $r_1, \cdots, r_n$ is

$$\langle r_1, \cdots, r_n \rangle := \{ r_1 s_1 + \cdots r_n s_n \mid s_i \in R \}.$$

It is clear that the ideal generated by $r_1, \cdots, r_n$ is the smallest ideal containing $r_1, \cdots, r_n$.

Definition 1.15. The produce of ideals I and J is the ideal which elements are of the form $i_1 j_1 + \cdots + i_n j_n$ for all $i_1, \cdots i_n \in I$, $j_1, \cdots, j_n \in J$.

For ideals I, J, we see that $IJ \subseteq I \cap J$ though they are not necessary equal (consider $\langle 2 \rangle \langle 2 \rangle = \langle 4 \rangle$ thought $\langle 2 \rangle \cap \langle 2 \rangle = \langle 2 \rangle$).

Proposition 1.10. If ideals I, J satisfy $I + J = \langle 1 \rangle$, then $I \cap J = IJ$.

As with other mathematical objects, we would like to construct a quotient object for the rings. The equivalence relation we shall quotient on it the following. Let $I \subseteq R$ be an ideal and we define say $r \equiv s \mod I$ for $r, s \in R$ if $r - s \in I$. It is not difficult to check that $\equiv_I$ is a equivalence relation and thus, we may take a quotient of R with respect to this equivalence relation and we denote the equivalence classes with $r + I$.

Definition 1.16 (Quotient Ring)**.** Given R a ring and I an ideal of R, then the quotient ring of R by I is the ring with the underlying set

$$R/I := R/ \equiv_I = \{ r + I \mid r \in R \},$$

where $0_{R/I} = 0_R + I$, $1_{R/I} = 1_R + I$, and for all $r + I, s + I \in R/I$, $(r+I) + (s+I) = (r+s) + I$ and $(r + I) \cdot (s + I) = rs + I$.

Definition 1.17 (Quotient Map)**.** Given R a ring and I an ideal of R, the quotient map is then the surjective ring homomorphism $q : R \to R/I : r \mapsto r + I$.

It is clear that $\ker q = I$.

A more modern interpretation of the quotient ring is by defining it as an object satisfying its universal property. In particular, the ring R/I, taken together with a ring homomorphism $q : R \to R/I$, has the following universal property.

Proposition 1.11. If $f : R \to S$ is a ring homomorphism such that $I \subseteq \ker f$, then there exists a unique ring homomorphism $\tilde{f} : R/I \to S$ such that for all $r \in R$, $\tilde{f}(r + I) = f(r)$.

Essentially, the universal property states that there exists a unique $\tilde{f}$ such that the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "q"'] & S \\ R/S \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Proof. Uniqueness is clear and thus we will show $\tilde{f}$ is well-defined and is a ring homomorphism. Let $r \equiv s \mod I$, and will show $f(r) = f(s)$. Indeed, since $r - s \in I$, we have $r - s \in \ker f$ and so, $f(r) - f(s) = f(r - s) = 0$, hence $f(r) = f(s)$ and $\tilde{f}$ is well-defined. Now, let $r + I, s + I \in R/I$, we have

$$\tilde{f}((r + I) + (s + I)) = \tilde{f}((r + s) + I) = f(r + s) = f(r) + f(s) = \tilde{f}(r + s) + \tilde{f}(s + I),$$

hence by similar argument for multiplication, we have $\tilde{f}$ is a ring homomorphism. $\square$

As an example consider the surjective map $\mathbb{R}[X] \to \mathbb{C}$ which is id on $\mathbb{R}$ and sends X to i. Then this map have kernel $\{P \in \mathbb{R}[X] \mid P(i) = 0\} = \langle X^2 + 1 \rangle$. Thus, we have the diagram

$$\begin{tikzcd}
\mathbb{R}[X] \arrow[r] \arrow[d, "q"'] & \mathbb{C} \arrow[dl] \\
\mathbb{R}[X]/\langle X^2+1 \rangle \arrow[ur] &
\end{tikzcd}$$

where the pull-back map is an isomorphism as the map itself is surjective while injectivity follows as we have quotiented out its kernel. As we shall see, whenever we have one field inside another, there is a construction similar this such that we can construct the larger field from the smaller field.

By recalling the evaluation map, if $\alpha \in R$, by the above process, we see that

$$R[X]/I \cong R[\alpha],$$

where I is the kernel of the evaluation map at α.

Definition 1.18. Let R be a ring and I an ideal of R. Then we say I is a prime ideal if R/I is an integral domain. Furthermore, we say I is a maximal ideal if R/I is a field.

Since fields are integral domains, maximal ideals are prime.

Proposition 1.12. An ideal I of R is prime if and only if for all $rs \in I$, either $r \in I$ or $s \in I$.

Proposition 1.13. An ideal I of R is maximal if and only if the only ideal of R containing I is I or the unit ideal R.

Proof. Follows by considering that a ring is a field if and only if its only ideals are the zero or the unit ideal, and the image of an ideal by a surjective homomorphism is also an ideal. $\square$

1.3 Factorization

Definition 1.19 (Unit)**.** Let R be a integral domain, then $R^\times$ is the set of elements r of R such that there exists some $r' \in R$ such that $rr' = 1$. If $r \in R^\times$, then we call r a unit.

Definition 1.20 (Divides)**.** Let $r, s \in R$, we say r divides s if $s \in \langle r \rangle$.

It is clear that a unit divides any element. Indeed, if $u \in R^\times$ and $s \in R$ such that $uu' = 1$, then $s = (su')u$ implying $s \in \langle u \rangle$.

Definition 1.21 (Associate)**.** An associate of $r \in R$ is an element ur of r with $u \in R^\times$.

Definition 1.22 (Irreducible)**.** An element $r \in R$ is irreducible if $r \neq 0$, $r \notin R^\times$ and the only dividors of r are units and associates of r.

Definition 1.23 (Unique Factorization Domain)**.** A ring R is a unique factorization domain (UFD) if it is a integral domain and

- for all non-zero, non-unit element of R is a product of finitely many irreducibles.

- for all $r \in R$ non-zero, non-unit such that

$$r = p_1 \cdots p_s = q_1 \cdots q_t,$$

where p_i, q_i are irreducibles, then $s = t$ and after reordering, p_i is an associate of q_i.

Some typical examples of UFDs are $\mathbb{Z}, \mathbb{F}[X], \mathbb{Z}[X], \cdots$ (where $\mathbb{F}$ is a field), though it is more challenging to come up with counter-examples. Consider the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, define

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z} : z \mapsto z\bar{z}.$$

It is easy to see that N is multiplicative, and thus, if $u \in \mathbb{Z}[\sqrt{-5}]$ is a unit such that $uu' = 1$, we have

$$N(u)N(u') = N(uu') = N(1) = 1,$$

implying $N(u) = \pm 1$ and so $u = \pm 1$. Then, as ± 1 are the only units of $\mathbb{Z}[\sqrt{-5}]$, we have $3 \cdot 2 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ are products of non-units which are not associate with each other. Hence, to show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD it suffices to show that the factors are irreducibles. To show this, one again use N by plugging the factors.

Let us construct a ring such that the first condition of UFD fails, i.e. a ring for which a non-zero, non-unit element is not a product of finitely many irreducibles. Define

$$\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}] := \left\{ \sum_{i=0}^{r} c_i t^{a_i} \mid c_i \in \mathbb{C}, a_i \in \mathbb{Q} \right\} = \bigcup_{n=1} \{ f^{1/n} \mid f \in \mathbb{C}[X] \}.$$

Then, $\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]^\times = \mathbb{C}^\times$ and in fact, $\mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]$ does not have any irreducible elements. Let $f \in \mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]^\times$ such that $f = P(t^{1/n})$ and $f^{-1} = Q(t^{1/m})$, then we may write $f = P'(t^{1/(nm)})$ and $f^{-1} = Q'(t^{1/(nm)})$. Hence,

$$1 = P'(t^{1/(nm)})Q'(t^{1/(nm)}) \implies P'Q' = 1 \implies P', Q' \text{ are constants},$$

and so $f \in \mathbb{C}^\times$. On the other hand, if $P(t^{1/n}) \in \mathbb{C}[t^{\mathbb{Q}_{\geq 0}}]$ is irreducible, by the fundamental theorem of algebra, it is a product of linear polynomials implying $P(t^{1/n}) = t^{1/n} - a$ for some $a \in \mathbb{C}$. But, $t^{1/n} - a = (t^{1/(2n)} + \sqrt{a})(t^{1/(2n)} - \sqrt{a})$, a contradiction.

Definition 1.24 (Prime)**.** An element r of a ring R is prime if $\langle r \rangle$ is a prime ideal. Equivalently, r is prime if for all $s, t \in R$, $r \mid st$ implies either $r \mid s$ or $r \mid t$.

Proposition 1.14. Let R be an integral domain in which every element is a finite product of irreducibles. Then every irreducible element of R is prime if and only if for all

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

where p_i, q_i are irreducible, then $s = t$ and after reordering, p_i is an associate of q_i.

Proof. Suppose every irreducible element of R is prime. Then, if

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

where p_i, q_i are irreducible, we have $p_1 \mid q_1, \cdots, q_t$ and so, $p_1 \mid q_i$ for some $i = 1, \cdots, t$, and hence p_i is an associate of q_1. Then, by reordering, we have p_1 and q_1 are associates. Repeating this argument, we may cancel all associates with some terms remaining if $s > t$,

$$p_{t+1} \cdots p_s = 1.$$

But this is a contradiction since then p_{t+1} is a unit and so $s = t$ as required.

Conversely, suppose r is irreducible and $r \mid st$ and so there exists some $rx = st$ for some $x \in R$. Then, we may factor x, s, t into irreducibles such that

$$rp_1 \cdots p_l = q_1 \cdots q_m n_1 \cdots n_k.$$

Then, as such factorizations are unique, r must be an associate of some q_i or n_i which implies that $r \mid s$ or $r \mid t$, so r is prime. □

Proposition 1.15. In an integral domain R, if $r \in R$ is prime, then r is irreducible.

Proof. Suppose otherwise, $r = st$. Then $r \mid st$ but neither $r \mid s$ nor $r \mid t$. □

A counter-example of the reverse is that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ but is not a prime.