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 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 $f \in F \setminus \{0_F\}$, 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 $P(X) \in \mathbb{Z}[X] \setminus \{0\}$, $P(\pi) \neq 0$. 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^2 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. □

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, $f(n_{\mathbb{Z}}) = n_{\mathbb{Z}} \cdot 1_R$. □

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 $P \in R[X]$. □

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 $I \cap J = IJ$.