

# Algebra III

Kexing Ying

July 24, 2021

## Contents

<b>1</b>	<b>Definitions</b>	<b>2</b>
1.1	Subrings and Extensions . . . . .	3

# 1 Definitions

We will in this section recall and introduce 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  $+_R, \times_R : R^2 \rightarrow R$  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  $r_0 + r_1\alpha + \dots + r_n\alpha^n$  for  $r_i \in S$  and  $n \in \mathbb{N}$ . We call this process the adjoining of  $S$  with  $\alpha$ .

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  $r_0 + r_1\alpha + \dots + r_n\alpha^n \in \mathbb{Z}[\alpha]$ ,

$$\begin{aligned} r_0 + r_1\alpha + r_2\alpha^2 + \dots + r_n\alpha^n &= r_0 + r_1\alpha + r_2(r\alpha + s) + \dots \\ &= (r_0 + r_2s + \dots) + (r_1 + r_2r + \dots)\alpha. \end{aligned}$$

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  $\pi$  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  $P(\pi) = r_0 + r_1\pi + \dots + r_n\pi^n = s_0 + s_1\pi + \dots + s_m\pi^m = Q(\pi)$ , WLOG.  $n \leq m$  we have  $0 = (s_0 - r_0) + (s_1 - r_1)\pi + \dots + (s_n - r_n)\pi^n + s_{n+1}\pi^{n+1} + \dots + s_m\pi^{m+1}$ , implying  $s_i = r_i$  for all  $i = 1, \dots, n$  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  $\alpha$ , 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  $\text{Frac}(R)$ , 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  $a/b, r/s \in \text{Frac}(R)$

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

It is routine to check these operations are well-defined and that the ring axioms are satisfied. Furthermore, as the name suggests,  $\text{Frac}(R)$  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  $\text{Frac}(R)$ .

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.