Week 8

Rings of polynomials

Definition. Let R be a nonzero commutative ring.

A **polynomial** with coefficients in R (in one-variable) is a formal sum

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

with $a_i \in R$ such that $a_i = 0$ for all but finitely many i's.

If $a_i \neq 0$ for some i, then the largest such i is called the **degree** of $f(x)$, denoted by $\deg f(x)$.

We denote by $R[x]$ the set of all polynomials with coefficients in R.

Given

$$f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x],$$

we define the addition and multiplication as follows (as usual):

$$f(x) + g(x) := \sum_{i=0}^{\infty} (a_i + b_i) x^i,$$

$$f(x)g(x) := \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i.$$

Proposition 8.0.1. *With addition and multiplication thus defined, $R[x]$ is a commutative ring.*

Proof. **Exercise.** □

Remark. A polynomial $f(x)$ defines a function $f : R \to R$ by $a \mapsto f(a)$. But $f(x)$ may not be determined by $f : R \to R$. For example, the polynomials

$$f(x) = 1 + x + x^2, g(x) = 1 \in \mathbb{Z}_2[x]$$

define the same (constant) function from $\mathbb{Z}_2$ to itself.

Integral domains and fields

Definition. A nonzero commutative ring R is called an **integral domain** if the product of two nonzero elements is always nonzero.

Definition. A nonzero element r in a ring R is called a **zero divisor** if there exists nonzero $s \in R$ such that $rs = 0$.

So a nonzero commutative ring R is an integral domain if and only if it has no zero divisors.

Example 8.0.2.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains, so are $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$. (More generally, if R is an integral domain, so is $R[x]$.)

2. Since $2, 3 \not\equiv 0 \mod 6$, and $2 \cdot 3 = 6 \equiv 0 \mod 6$, the ring $\mathbb{Z}_6$ is not an integral domain.

3. Consider $R = C[-1, 1]$, the ring of all continuous functions on $[-1, 1]$, equipped with the usual operations of addition and multiplication for functions. Let:

$$f = \begin{cases} -x, & x \leq 0, \\ 0, & x > 0. \end{cases} \quad , \quad g = \begin{cases} 0, & x \leq 0, \\ x, & x > 0. \end{cases}$$

Then f and g are nonzero elements of R, but $fg = 0$. So R is not an integral domain.

Proposition 8.0.3. *A commutative ring R is an integral domain if and only if the cancellation law holds for multiplication, i.e. whenever $ca = cb$ and $c \neq 0$, we have $a = b$.*

Proof. Suppose R is an integral domain. If $ca = cb$, then by distributive laws, $c(a - b) = c(a + -b) = 0$. Since R is an integral domain, we have either $c = 0$ or $a - b = 0$. So, if $c \neq 0$, we must have $a = b$.

Conversely, suppose cancellation law holds. Suppose there are nonzero $a, b \in R$ such that $ab = 0$. By a previous result we know that $0 = a0$. So, $ab = a0$, which by the cancellation law implies that $b = 0$, a contradiction. □

Definition. Let R be a ring. We say that an element $a \in R$ is a **unit** if it has a multiplicative inverse, i.e. there is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Example 8.0.4. The only units of $\mathbb{Z}$ are ± 1.

Example 8.0.5. Let R be the ring of all real valued functions on $\mathbb{R}$. Then, any function $f \in R$ satisfying $f(x) \neq 0, \forall x$, is a unit.

Example 8.0.6. Let R be the ring of all continuous real valued functions on $\mathbb{R}$, then $f \in R$ is a unit if and only if it is either strictly positive or strictly negative.

Proposition 8.0.7. *The only units of $\mathbb{Q}[x]$ are nonzero constants.*

Proof. Given any $f \in \mathbb{Q}[x]$ such that $\deg f > 0$, for all nonzero $g \in \mathbb{Q}[x]$ we have

$$\deg fg \geq \deg f > 0 = \deg 1;$$

hence, $fg \neq 1$. If $g = 0$, then $fg = 0 \neq 1$. So, f has no multiplicative inverse.

If f is a nonzero constant, then $f^{-1} = \frac{1}{f}$ is a constant polynomial in $\mathbb{Q}[x]$, and $f\left(\frac{1}{f}\right) = \left(\frac{1}{f}\right) f = 1$. So, f is a unit.

Finally, if $f = 0$, then $fg = 0 \neq 1$ for all $g \in \mathbb{Q}[x]$, so the zero polynomial has no multiplicative inverse. □

Definition. A **field** is a commutative ring, with $1 \neq 0$, in which every nonzero element is a unit.

In other words, a nonzero commutative ring F is a field if and only if every nonzero element $r \in F$ has a multiplicative inverse r^{-1}, i.e. $rr^{-1} = r^{-1}r = 1$.

Example 8.0.8. 1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

2. The polynomial rings $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ are not fields.

Note that if every nonzero element of a commutative ring has a multiplicative inverse, then that ring is an integral domain:

$$ca = cb \implies c^{-1}ca = c^{-1}cb \implies a = b.$$

So we conclude that

Proposition 8.0.9. *A field is an integral domain.*

Proposition 8.0.10. *Let $k \in \mathbb{Z}_m \setminus \{0\}$.*

- *If $\gcd(k, m) > 1$, then k is a zero divisor.*
- *If $\gcd(k, m) = 1$, then k is a unit.*

Proof. Let $d := \gcd(k, m)$.

If $d > 1$, then m/d is a nonzero element in $\mathbb{Z}_m$, and we have $k \cdot_m (m/d) = \overline{(k/d) \cdot m} = 0$ in $\mathbb{Z}_m$. So k is a zero divisor.

If $d = 1$, then there exist $a, b \in \mathbb{Z}$ such that $ak + bm = 1$. But this means we have $\overline{a}k = 1$ in $\mathbb{Z}_m$. So k is a unit. □

Hence, the set of zero divisors in $\mathbb{Z}_m$ is precisely given by

$$\{k \in \mathbb{Z}_m \setminus \{0\} : \gcd(k, m) > 1\}$$

and the set of units in $\mathbb{Z}_m$ is precisely given by

$$\mathbb{Z}_m^\times := \{k \in \mathbb{Z}_m \setminus \{0\} : \gcd(k, m) = 1\}.$$

In particular, we have the following

Corollary 8.0.11. *$\mathbb{Z}_m$ is a field if and only if m is prime.*

Notation. For p prime, we often denote the field $\mathbb{Z}_p$ by $\mathbb{F}_p$.

Proposition 8.0.12. *Equipped with the usual operations of addition and multiplications for real numbers, $F = \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a field.*

Proof. Observe that: $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$ lies in F, and $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in F$. Hence, addition and multiplication for real numbers are well-defined operations on F. As operations on $\mathbb{R}$, they are commutative, associative, and satisfy the distributive laws; therefore, as F is a subset of $\mathbb{R}$, they also satisfy these properties as operations on F.

It is clear that 0 and 1 are the additive and multiplicative identities of F. Given $a + b\sqrt{2} \in F$, where $a, b \in \mathbb{Q}$, it is clear that its additive inverse $-a - b\sqrt{2}$ also lies in F. Hence, F is a commutative ring.

To show that F is a field, for every nonzero $a + b\sqrt{2}$ in F, we need to find its multiplicative inverse. As an element of the field $\mathbb{R}$, the multiplicative inverse of $a + b\sqrt{2}$ is:

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}}.$$

It remains to show that this number lies in F. Observe that:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

We claim that $a^2 - 2b^2 \neq 0$. Suppose $a^2 - 2b^2 = 0$, then either (i) $a = b = 0$, or (ii) $b \neq 0$, $\sqrt{2} = |a/b|$. Since we have assumed that $a + b\sqrt{2}$ is nonzero, case (i) cannot hold. But case (ii) also cannot hold because $\sqrt{2}$ is know to be irrational. Hence $a^2 - 2b^2 \neq 0$, and:

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2},$$

which lies in F. □

Proposition 8.0.13. *All finite integral domains are fields.*

Proof. Let R be an integral domain with n elements, where n is finite. Write $R = \{a_1, a_2, \ldots, a_n\}$. We want to show that for any nonzero element $a \neq 0$ in R, there exists i, $1 \leq i \leq n$, such that a_i is the multiplicative inverse of a. Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. Since R is an integral domain, the cancellation law holds. In particular, since $a \neq 0$, we have $aa_i = aa_j$ if and only if $i = j$. The set S is therefore a subset of R with n distinct elements, which implies that $S = R$. In particular, $1 = aa_i$ for some i. This a_i is the multiplicative inverse of a. □

Field of Fractions (optional)

An integral domain fails to be a field precisely when there is a nonzero element with no multiplicative inverse. The ring $\mathbb{Z}$ is such an example, for $2 \in \mathbb{Z}$ has no multiplicative inverse. But any nonzero $n \in \mathbb{Z}$ has a multiplicative inverse $\frac{1}{n}$ in $\mathbb{Q}$, which is a field. So, a question one could ask is, can we "enlarge" a given integral domain to a field, by formally adding multiplicative inverses to the ring?

An Equivalence Relation

Given an integral domain R (commutative, with $1 \neq 0$). We consider the set: $R \times R_{\neq 0} := \{(a, b) : a, b \in R, b \neq 0\}$. We define a relation $\equiv$ on $R \times R_{\neq 0}$ as follows:

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

Lemma 8.0.14. *The relation $\equiv$ is an equivalence relation.*

In other words, the relation $\equiv$ is:

Reflexive: $(a, b) \equiv (a, b)$ for all $(a, b) \in R \times R$

Symmetric: If $(a, b) \equiv (c, d)$, then $(c, d) \equiv (a, b)$.

Transitive: If $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then $(a, b) \equiv (e, f)$.

Proof. **Exercise.** □

In general, given an equivalence relation $\sim$ on a set S, the **equivalent class** of an element $a \in S$ is the set of all elements in $s \in S$ which are equivalent to a (i.e. $s \sim a$).

Notation: For notational convenience, to describe an equivalence class we may pick any element s (called a **representative**) belonging to the class, and label the class as $[s]$. Note that if $s \sim t$, then $[s] = [t]$.

Due to the properties (reflexive, symmetric, transitive), of an equivalence relation, the equivalent classes form a **partition** of S. Namely, equivalent classes of non-equivalent elements are disjoint:

$$[s] \cap [t] = \varnothing$$

if $s \not\sim t$; and the union of all equivalent classes is equal to S:

$$\bigcup_{s \in S} [s] = S.$$

Definition. Given an equivalence relation $\sim$ on a set S, the **quotient set** $S/\sim$ is the set of all equivalence classes of S, with respect to $\sim$.

We now return to our specific situation of $R \times R_{\neq 0}$, with $\equiv$ defined as above. We define addition $+$ and multiplication $\cdot$ on $R \times R_{\neq 0}$ as follows:

$$(a, b) + (c, d) := (ad + bc, bd)$$
$$(a, b) \cdot (c, d) := (ac, bd)$$

Proposition 8.0.15. *Suppose* $(a, b) \equiv (a', b')$ *and* $(c, d) \equiv (c', d')$*, then:*

1. $(a, b) + (c, d) \equiv (a', b') + (c', d')$.
2. $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$.

Proof. By definition, $(a, b) + (c, d) = (ad + bc, bd)$, and $(a', b') + (c', d') = (a'd' + b'c', b'd')$. Since by assumption $ab' = a'b$ and $cd' = c'd$, we have:

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'bdd' + c'dbb' = (a'd' + b'c')bd;$$

hence, $(a, b) + (c, d) \equiv (a', b') + (c', d')$.

For multiplication, by definition we have $(a, b) \cdot (c, d) = (ac, bd)$ and $(a', b') \cdot (c', d') = (a'c', b'd')$. Since

$$acb'd' = ab'cd' = a'bc'd = a'c'bd,$$

we have $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$. □

Let:

$$\mathrm{Frac}(R) := (R \times R_{\neq 0})/\equiv,$$

and define $+$ and $\cdot$ on $\mathrm{Frac}(R)$ as follows:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

Corollary 8.0.16. *$+$ and $\cdot$ thus defined are well-defined binary operations on* $\mathrm{Frac}(R)$.

Namely, we get the same output in $\mathrm{Frac}(R)$ regardless of the choice of representatives of the equivalence classes.

Proposition 8.0.17. *The set* $\mathrm{Frac}(R)$*, equipped with $+$ and $\cdot$ defined as above, forms a field, with additive identity* $0 = [(0,1)]$ *and multiplicative identity* $1 = [(1,1)]$*. The multiplicative inverse of a nonzero element* $[(a,b)] \in \mathrm{Frac}(R)$ *is* $[(b,a)]$.

Proof. **Exercise.** □

Definition. $\mathrm{Frac}(R)$ is called the **Fraction Field** of R.

Remark. Note that $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, if we identify $a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, with $[(a,b)] \in \mathrm{Frac}(\mathbb{Z})$.