Part IV (§18-24)
Rings and Fields

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

18 Rings and Fields

Groups dealt with only one binary operation.
You are used to working with two binary operation,
in the usual objects you work with: $\mathbb{Z}, \mathbb{R}$.
Now we will study with such objects,
with two binary operations: additions and multiplication.

18.1 Defintions and Basic Properties

Definition 18.1. *A* **Ring** $\langle R, +, \cdot \rangle$ *is a set with two binary operations* $+, \cdot$, *which we call addition and multiplication, defined on* R *such that*

1. $\langle R, +, \cdot \rangle$ *is an abelian group. The additive identiy is denoted by zero* 0.
2. *Multiplication is associative.*
3. *The distributive property is satiesfied as follows:*

$$\forall\ a, b, c \in R \quad a(b+c) = ab + ac \quad \textit{and} \quad (b+c)a = ba + ca.$$

Further, A ring $\langle R, +, \cdot \rangle$ is called a **commutative ring**, *if the multiplication is commutative. That means, if*

$$\forall\ a, b \in R \quad ab = ba.$$

Definition 18.2. *Let $\langle R, +, \cdot \rangle$ be a ring. If R has a multiplicative identity, then we has $\langle R, +, \cdot \rangle$ is a* **ring with unity**. *The multiplicative unit is denoted by* 1. *Recall, it means*

$$\forall\ x \in R \qquad 1 \cdot x = x \cdot 1 = x.$$

Barring some exceptions (if any), **we consider rings with unity only**.

Lemma 18.3. *Suppose $\langle R, +, \cdot \rangle$ is a ring with unity. Suppse $0 = 1$. then $R = \{0\}$.*

Proof. Suppose $x \in R$. Then,

$$x = x \cdot 1 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 = x \cdot 1 + x \cdot 1 = x + x.$$

So, $x + x = x$ and hence $x = 0$. So, $R \subseteq \{0\}$ and hence So, $R = \{0\}$. The proof is complete. ∎

Remark. The ring $R = \{0\}$ is not interesting. So, we consider $R \neq \{0\}$ only. Hence we will always have $0 \neq 1$.

Example 18.4 (18.2)**.** Following are rings:

$$\langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{Q}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle, \langle \mathbb{C}, +, \cdot \rangle$$

Example 18.5 (18.3)**.** Let R be any ring. Then, the set $M_n(R)$ of all square matrices, with coefficients in R is a ring under the matrix addition and matrix multiplication.

1. **Question:** What is the additive identity of $M_n(R)$?
2. **Question:** What is the multiplicative identity of $M_n(R)$?

In particular

$$M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R}), M_n(\mathbb{C}) \qquad \textit{are rings.}$$

Remark. For $n \geq 2$ these rings are not commutative. In group theory, we gave examples.

Example 18.6 (18.4)**.** Let F be a set of all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$. For $f, g \in F$ define addition and multiplication as follows:

$$(f+g)(x) = f(x) + g(x) \qquad \textit{and} \qquad (fg)(x) = f(x)g(x)$$

Then, F is a ring under this addition and multiplication.

1. **Question:** What is the additive identity of this ring?
2. **Question:** What is the multiplicative identity of this ring?

Example 18.7 (18.6)**.** For any integer $n > 0$, $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring.

Example 18.8 (18.7)**.** Let $R_1, R_2, \cdots, R_n$ be n rings. Then, the direct product $R := R_1 \times R_2 \times \cdots \times R_n$ is a ring. For $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R$ addition and multiplication is defined by

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

Theorem 18.9. *Let R be a ring and $a, b \in R$. Then,*

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$.

Proof. First, $-a$ is the notation for the additive inverse of a. The proofs are routine:

1. $0a = (0+0)a = 0a + 0a$. Subtracting $0a$ (i.e. adding $-(0a)$) from both sides we have $0a = 0$. Similarly $a0 = 0$.

2. We have $(ab)+a(-b) = a(b-b) = b0 = 0$. So, $-(ab) = a(-b)$. Similarly, $-(a) = (-a)b$.

3. We have, by (2), $(-a)(-b) = -((a(-b)) = -(-(ab)) = ab$.

The proof is complete. ∎

18.2 Homomorphisms

As always, homomophism of two object with certain structure, is a mapping that respects the structure.

Definition 18.10. *Let R, R' be two rings.*

1. *A map $\varphi : R \longrightarrow R'$ is said to be a* **homomorphism** *if, for all $a, b \in R$ we have*
   (a) $\varphi(a+b) = \varphi(a) + \varphi(b)$
   (b) $\varphi(ab) = \varphi(a)\varphi(b)$
   (c) We also assume $\varphi(1) = 1$.
2. *A homomorphism $\varphi : R \longrightarrow R'$ is said to be an isomorphism, if it is also bijective.* (I do not like this definition. Will clarify in class).

Example 18.11. As in (18.6), let F be the ring of all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$. Let $a \in \mathbb{R}$. Then, the evaluation at $a \in \mathbb{R}$ is a homomorphism, defined as:

$$\varphi_a : F \longrightarrow \mathbb{R} \qquad defines\ as \quad \varphi_a(f) = f(a).$$

Example 18.12. The mapping

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n \qquad given\ by \quad \varphi(x) = \overline{x}$$

is a homomorphism of rings.

Lemma 18.13. *Let $\varphi : R \longrightarrow R'$ be an isomorphism of rings. Since φ is bijective, it has a set theoretic inverse $\varphi^{-1} : R' \longrightarrow R$. In fact, φ^{-1} is also an isomorphism* (that mweans a homomorphisn, in addition to being a bijection.).

Proof. *Let $y_1, y_2 \in R'$, we need to prove that*

$$\varphi^{-1}(y_1 + y_2) = \varphi^{-1}(y_1) + \varphi^{-1}(y_2) \quad \textit{and} \quad \varphi^{-1}(y_1 y_2) = \varphi^{-1}(y_1)\varphi^{-1}(y_2)$$

Since φ is injective, it is enough to prove that they are equal after an application of φ. In deed

$$y_1 + y_2 = \varphi(\varphi^{-1}(y_1) + \varphi^{-1}(y_2)) \quad \textit{and} \quad y_1 y_2 = \varphi(\varphi^{-1}(y_1)\varphi^{-1}(y_2)).$$

The proof is complete. ∎

18.3 Multiplicative Questions: Fields

Notations 18.14. Let R be a ring with unity (as always). Then, there is a homomorphism

$$\varphi : \mathbb{Z} \longrightarrow R \qquad \textit{defined by} \quad \forall n \geq 0 \quad \varphi(n) = 1 + 1 + \cdots + 1 (n \textit{ summands})$$

and $\varphi(-n) = -\varphi(n)$. We use the notation

$$n := \varphi(n) \in R \qquad \textit{and} \quad \textit{also} \quad n \cdot 1 := \varphi(n).$$

(You can call φ the premitive homomorphims or cannonical homomorphism. In the category of rings with unit, $\mathbb{Z}$ is considered as the innitial object, for this reason.)

Example 18.15 (18.15)**.** Let r, s be positive integers with $\gcd(r, s) = 1$. Then

$$\varphi : \mathbb{Z}_r \times \mathbb{Z}_s \longrightarrow \mathbb{Z}_{rs} \qquad \textit{given by} \quad \varphi(n \cdot 1) = n \cdot (1, 1)$$

is an isomorphism. Note, both sides are cyclic groups.

Definition 18.16. *Let R be a ring with $1 \neq 0$.*

1. *An element $u \in R$ is called an* **unit**, *if u has a multiplicative inverse in R. Note, zero 0 cannot be an unit (why?).*
2. *We say R is a* **division ring** *(or* **skew field**), *if each nonzero element in R is an unit.*
3. *We say R is a* **field**, *if it is a division ring and if R is commutative.*

Example 18.17 (18.17)**.** What are the units of $\mathbb{Z}_n$? Answer: all $\overline{r}$ such that $\gcd(r, n) = 1$.

(See §20).

Example 18.18 (18.18)**.** A few examples of fields:

1. $\mathbb{Z}$ is not a field. Why not? What are the units of $\mathbb{Z}$?
2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.
3. At this time I do not have too many examples of a division ring that is not a field. I will write down the example of Quaternion Algebra, on the board.

Definition 18.19.

1. Suppose R is a ring. A **subring** of R is a subset S of R, such that S is ring under the addition and multiplication inherited from R.
2. Let E be a field. A **subfield** of E is a subset F of E, such that

   F is field under the addition and multiplication inherited from F.
3. So, $\mathbb{Z}$ is a subring of $\mathbb{R}$. $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
4. Such "sub"-structues are defined routinely in mathematics, whenever some kind of structures are defined.

(a) For example, we define subspaces W of vector spaces.

(b) We define subgroups.

(c) In topology, we define subspaces of topological spaces.

(d) Differential topology, we define submanifold N of a given manofold. For example, the unit disc is a submanifold of $\mathbb{C}$.

19 Integral Domains

In $\mathbb{Z}$, $ab = 0 \Longrightarrow a = 0$ *or* $b = 0$.

Example 19.1 (19.1)**.** Consider the ring $\mathbb{Z}_{12}$.

1. Here $\overline{3} \cdot \overline{4} = 0$ but none of the factors are zero.

2. Consider the equation $(x-2)(x-3) = 0$. Its solutions in $\mathbb{Z}_{12}$ are $\overline{2}, \overline{3}, \overline{6}, \overline{11}$.

   This is strange because, we are used to the idea that quadratics should have at most two root. Such strange things happen, because in this ring product of two nonzero elements can be zero.

Definition 19.2. *We give two definitions.*

1. *Let R be a ring. Let $a \in R$. We say that a is a* **zero divisor***, if $a \neq 0$ and $\exists\ b \in R$ with $b \neq 0$ such that $ab = 0$.*

2. *A commutative ring D is called an* **integral domain***, if D does not have any zero divizor.*

   So, a cmmutative ring R is an integral domain if and only if

$$\forall\ a, b \in D \quad (ab = 0 \Longrightarrow a = 0 \text{ or } b = 0).$$

Theorem 19.3. *Consider the ring $\mathbb{Z}_n$. An element $\overline{r} \in \mathbb{Z}_n$ is a zero divisor if and only if $gcd(r, n) \neq 1$* (i.e. r, n are NOT relatively prime)*.*

Proof. Suppose $\overline{r} \in \mathbb{Z}_n$.

1. ($\Leftarrow$): Suppose $gcd(r, n) = d \neq 1$ or $d \geq 2$, So, $r = dr_0, n = dn_0$ with $1 \leq n_0 \leq n-1$. So, $rn_0 = dn$ and $\overline{r}\ \overline{n_0} = 0$. Since, $\overline{n_0} \neq 0$, $\overline{r}$ is a zero divisor.

2. ($\Rightarrow$): Suppose $\overline{r}$ is a zero divisor. So, there is $0 \leq m \leq n-1$ such that $\overline{r}\ \overline{m} = 0$. So, n divides rm. If $gcd(r,n) = 1$ then it follows that n divides m, and so $\overline{m} = 0$. This is a contradiction. So, $gcd(r,n) \neq 1$.

The proof is complete. ■

Definition 19.4. *Suppose R is a commutative ring. We say that* **cancellation law holds** *in R if*

$$for\ a,b,c \in R\ \ with\ a \neq 0 \qquad (ab = ac \quad \Longrightarrow \quad b = c).$$

Theorem 19.5. *Let R be commutative ring. Then, R is an integral domain if and only if cancellation law holds in R.*

Proof. ($\Rightarrow$): Suppose R is an integral domain. Suppose

$$for\ some\ a,b,c \in R\ \ with\ a \neq 0 \qquad ab = ac.$$

Then, $a(b-c) = 0$. Since $a \neq 0$ we have $b - c = 0$ or $b = c$. So, the cancellation holds.

($\Leftarrow$): Suppose cancellation holds. Suppose $ab = 0$ and $a \neq 0$ for some $a, b \in R$. So, $ab = a0$. By cancellation $b = 0$. So, a is not a zero divisor. So, R has no zero divisor and R is an integral domain. The proof is complete. ■

Example 19.6 (19.7)**.** Few examples:

1. $\mathbb{Z}$ is an integral domain.
2. $\mathbb{Z}_p$ is an integral domain, if p is prime.
3. $\mathbb{Z}_n$ is NOT and an integral domain, unless n is a prime.
4. Let F be the ring of all continuous real valued functions on $\mathbb{R}$. Then, F is NOT and an integral domain. (why not?)
5. Let R, S be two rings. Then the direct product $R \times S$ NOT and an integral domain. This is because $(1,0)(0,1) = (0,0)$.

Example 19.7 (19.8)**.** Let R be any commutative ring. Then, $M_2(\mathbb{R})$ is NOT and an integram domain. This is because $M_2(\mathbb{R})$ is not commutative.

Theorem 19.8. *Every field F is an integral domain.*

Proof. Let $a \in F$ and $a \neq 0$. Suppose $ab = 0$. Since a has an inverse $a^{-1}(ab) = a^{-1}0 = 0$ gives $b = 0$. So, F is an integral domain. The proof is complete. ∎

Theorem 19.9. *Every finite integral domain R is a field.*

Proof. Write $R = \{0, 1, a_1, a_2, \ldots, a_n\}$. Suppose $a \in R$ and $a \neq 0$. We need to show that a has an inverse. Consider the list:

$$a1, aa_1, aa_2, \ldots, aa_n.$$

Since cancellation holds ths is a list are $n+1$ DISTINCT non zero elements in R. But R has only $n+1$ distinct elements, including 1. So, one of them must be 1 or $aa_r = 1$ for some r. So, a has an inverse. The proof is complete. ∎

Corollary 19.10. *$\mathbb{Z}_p$ is a field, when p is a prime.*

Proof. Exercise.

Definition 19.11. *Let R ba a ring with unity 1 (as always). If $n \cdot 1 \neq 0$ for all integers $n \geq 2$, we say R has* **characteristic zero**. *If $n \cdot 1 = 0$ for some integer $n \geq 2$ then the the* **characteristic** *is defined to be*

$$char(R) = \min\{n \geq 2 : n \cdot 1 = 0\}.$$

So, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ have characteristic zero. $\mathbb{Z}_n$ has characteristic n.

Theorem 19.12. *Let R be a ring of characteristic n. Then $n \cdot a = 0$ $\forall a \in R$.*

Proof. We have $n \cdot 1 = 0$. So, for $a \in R$ we have $n \cdot a = (n \cdot 1)a = 0 \cdot a = 0$ The proof is complete. ∎

20 Farmat's and Euler's Theorem

In this section we do some number game.

Lemma 20.1. *Let F be a field and F^* be the set of all nonzero elements in F. Then F^* is a group under multiplication.*

Proof. Trivial. ∎

Theorem 20.2 (Little Theorem of Fermat)**.** *Let p be a prime number and $a \in \mathbb{Z}$ be an integer that is not divisible by p. Then,*

$$a^{p-1} \equiv 1 \qquad (modulo\ p).$$

Proof. Since $\mathbb{Z}_p$ is a field,

$$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

is a group under multiplication. This group has order $p-1$. So, $\forall x \in \mathbb{Z}_p^*$ we have $x^{p-1} = \overline{1}$. So, $\overline{a}^{p-1} = \overline{1}$. This means,

$$a^{p-1} \equiv 1 \qquad (modulo\ p).$$

The proof is complete. ∎

Corollary 20.3. *For $a \in \mathbb{Z}$ and prime number p we have $a^p \equiv a \quad (modulo\ p)$.*

Proof. If a is divisible by p then $a^p \equiv a \equiv 0 \quad (modulo\ p)$. If a is not divisible by p then by the above theorem

$$a^{p-1} \equiv 1 \qquad (modulo\ p).$$

and so

$$a^p \equiv a \qquad (modulo\ p).$$

The proof is complete. ∎

Example 20.4 (20.3)**.** We compute the remainder of 8^{103} when devided by 13.

First, $108 = 12 * 8 + 7$. So,

$$8^{103} = (8^{12})^8 8^7 \equiv 1^8 8^7 \equiv (-5)^7 \equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \quad (modulo\, 13).$$

So, the remainder would be 5.

Example 20.5 (20.4)**.** Show $2^{11,213} - 1$ is not divisible by 11.

First, we will do (*modulo* 11) computations. So, divide the exponent by 10: we have $11,213 = 1121 * 10 + 3$. So,

$$2^{11,213} - 1 \equiv (2^{10})^{1121} 2^3 - 1 = 1^{1121} 8 - 1 \equiv 7 \quad (modulo\ 11).$$

Example 20.6 (20.5)**.** For any integer n, the number $n^{33} - n$ is divisible by 15.

Proof. We will show it is divisible by 3 and 5. First, we do (*modulo* 3) computation:

$$n^{33} - n \equiv (n^2)^{16} n - n = 1^{32} n - n = 0(modulo\ 3).$$

Now, we do (*modulo* 5) computat ion:

$$n^{33} - n \equiv (n^4)^8 n - n = 1^8 n - n = 0(modulo\ 5).$$

The proof is complete. ∎

20.1 Euler's Generalization

Theorem 20.7. *Let G_n be the nonzero divizors of $\mathbb{Z}_n$. Then G_n forms a group under multiplication.*

Proof. First, G_n is closed under multiplication: Let $x, y \in G_n$. Then $xy \neq 0$. Then

$$(xy)z = 0 \Longrightarrow yz = 0 \Longrightarrow z = 0.$$

So, $xy \in G_n$, meaning it is a nonzero divizor. Obviously, $1 \in G_n$. We need to prove that, each element in G_n has an inverse. The proof of this part is exactly similar to the proof of (19.9). (Complete it.) The proof is complete.■

Corollary 20.8. *If $\overline{r} \in \mathbb{Z}_n$ is a nonzero divisor, then it is invertible. So,*

$$G_n = \{\overline{r} \in \mathbb{Z}_n : 1 \leq r \leq n-1, \text{ and } \gcd(r,n) = 1.\}$$

Proof. The first statement is immediate from the theorem. For the second statement note, that $\overline{r} \in \mathbb{Z}_n$ is invertible if and only id $\gcd(r,n) = 1$. The proof is complete. ■

Definition 20.9. *For integers $n \geq 1$, let $\varphi(n)$ be defined as the number of integers $1 \leq r \leq n-1$ such that $\gcd(r,n) = 1$. So,*

$$\varphi(n) = |G_n|.$$

Theorem 20.10 (Euler's Theorem)**.** *For any integer a, relatively prime to n we have*

$$a^{\varphi(n)} \equiv 1 \qquad (\textit{modulo } n).$$

Proof. For such an integer a, the element $\overline{a} \in G_n$. Since order of G_n is $\varphi(n)$, we have $\overline{a}^{\varphi(a)} = \overline{1}$. This means,

$$a^{\varphi(n)} \equiv 1 \qquad (\textit{modulo } n).$$

Example 20.11 (20.9)**.** Let $n = 12$. Then, $1, 5, 7, 11$ the positive integers less than 12 that are relatively prime to 12. So, $\varphi(12) = 4$.

So, for any integer a, relatively prime to 12, we have

$$a^4 \equiv 1 \qquad (modulo\ 12).$$

For example $3025 = 5^2 11^2$ is relatively prime to 12. So,

$$(3025)^4 \equiv 1 \qquad (modulo\ 12).$$

20.2 Application to $ax \equiv b \pmod{m}$

Theorem 20.12. *Let m be a positive intger and let $a \in \mathbb{Z}_m$ be relatively prime to m. Then for each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution.*

Proof. It follows, a has an inverse in $\mathbb{Z}_m$. So, $x = a^{-1}b$ is the unique solution. The proof is complete. ∎

This theorem can be restated as follows.

Corollary 20.13. *If a, m are relatively prime integers, then for any integer b, the equation*

$$ax \equiv b \qquad (modulo\ m)$$

has solutions. Further all solutions are in the same equivalence class. Namely solutions are the member of the class $\overline{a}^{-1}\overline{b}$.

We skip the rest of the section. It is becoming technical.

21 The Field of Quotients of an Integral Domain

Soppose D is an integral domain. We want to enlarge D to a field, by adding inverses of all the nonzero elements of D. In a sense, we repeat the process how, we get the field of rationals $\mathbb{Q}$, by adding inverses of nonzero elements in $\mathbb{Z}$.

21.1 The construction

Let D be an integral domain.

1. Consider the set
$$S = \{(a, b) : a, b \in D, b \neq 0\}$$
We will define an equivalence relation, so that the equivalence class of (a, b) will represent a/b. Intuitively, think of (a, b) as a representation of a/b.

2. Define a relationship as follows:

Definition 21.1. *For $(a, b), (c, d) \in S$, define*

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

Lemma 21.2. The relation $\sim$ is an equivalence relation.

Proof. We check the three conditions:

(a) (**Reflexive**): For all $(a, b) \in S$ we have $(a, b) \sim (a, b)$ because $ab = ba$.

(b) (**Symmetric**): Suppose $(a, b) \sim (c, d)$. Then, $ad = bc$. So, $cb = ad$ and hence $(c, d) \sim (a, b)$.

(c) (**Transitive**): Suppose $(a, b) \sim (c, d) \sim (u, v)$. Then, $ad = bc$ and $cv = du$. So, $(ad)u = (bc)u$ or $a(du) = bcu$ or $a(cv) = bcu$. Cancelling c we get or $av = bu$. So, $(a, b) \sim (u, v)$. So, the relation is transitive.

So, it is established that $\sim$ is an equivalence. The proof is complete. ■

3. The set of all equivalence classes will be denoted by F and the equivalence class of (a, b) will be denoted by $[(a, b)]$. So,

$$F = \{[(a, b)] : (a, b) \in S\}.$$

4. Intuitively, we think
$[(a, b)] =: \frac{a}{b}$ and define addition and multiplication of equivalence classes, in F, as in the lemma.

Lemma 21.3. For $[(a, b)], [(c, d)] \in F$ define

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)] \quad \textit{and} \quad [(a, b)][(c, d)] := [(ac, bd)]$$

We assert that these are well-define operations (to be called addition and multiplication).

Proof. First, since $(a, b), (c, d) \in S$, we have $b \neq 0, d \neq 0$. Since D is an integral domain, $bd \neq 0$. So, $(ad + bc, bd) \in S$ and $(ac, bd) \in S$. So, the right handsides are in F, or F is closed under additing and multiplication.

We need to prove well defined-ness. Suppose $[(a, b)] = [(a_1, b_1)]$ and $(c, d) = (c_1, d_1)$. That means, $(a, b) \sim (a_1, b_1)$ and $(c, d) \sim (c_1, d_1)$. So,

$$ab_1 = ba_1, cd_1 = dc_1 \qquad (*).$$

Multiply thse two equations, we get

$$ab_1cd_1 = ba_1dc_1. \qquad So, (ac, bd) \sim (a_1c_1, b_1d_1).$$

So, the multiplication is well defined. (*I am "thinking" fractions a/b and so on.*)

For addition, I want "common denominators" (the second coordinate): So, multiply the first equation by dd_1 and the second equation by bb_1. We have

$$ab_1dd_1 = ba_1dd_1, cd_1bb_1 = dc_1bb_1$$

Adding, we get

$$(ad+cb)b_1d_1 = (a_1d_1+c_1b_1)db. \quad So, \quad (ad+cb, bd) \sim (a_1d_1+c_1b_1, b_1d_1).$$

So, the addition is well defined. The proof is complete. ■

5. **Notation.** Now on, we will use the notation

$$a/b = \frac{a}{b} := [(a, b)].$$

6. Now, we prove F is a field.

   (a) $\langle F, + \rangle$ is a abelian group. **Proof.**

      i. We have

      $$([(a, b)]+[(c, d)])+[(x, y)] = [(ad+bc, bd)]+[(x, y)] = [(ady+bcy+bdx, bdy)]$$

      Similarly,

      $$[(a, b)] + ([(c, d)] + [(x, y)]) = [(ady + bcy + bdx, bdy)].$$

      $$So, \quad ([(a, b)] + [(c, d)]) + [(x, y)] = ([(a, b)] + [(c, d)]) + [(x, y)].$$

      So, the addition is associative.
      Alternately, If we are comfortable using the notations above, then

      $$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{x}{y} = \frac{ad + bc}{bd} + \frac{x}{y} = \frac{ady + bcy + bdx}{bdy}.$$

      Similarly,

      $$\frac{a}{b} + \left(\frac{c}{d} + \frac{x}{y}\right) = \frac{a}{b} + \frac{cy + dx}{dy} = \frac{ady + bcy + bdx}{bdy}.$$

      ii. We have

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

      So, the addition is commutative.

      iii. $[(0, 1)]$ is the additive identity (zero):

      $$[(0, 1)] + [(a, b)] = [(a, b)] = [(a, b)] + [(0, 1)]$$

      In fact, $[(0, 1)] = [(0, d)]$ for all $d \neq 0 \in D$.

      iv. The additive inverse of $[(a, b)] = [(-a, b)]$, because

      $$[(a, b)] + [(-a, b)] = [(0, b)].$$

This completes th eproof that $\langle F, + \rangle$ is a abelian group.

(b) The multiplication is associative, with an unity.

Proof.

i. (Associativity)

$$([(a,b)][(c,d)])[(x,y)] = [(ac,bd)][(x,y)]$$

$$= [(acx,bdy)] = [(a,b)]([(c,d)][(x,y)]).$$

ii. The multiplicative identity is $((1,1)] = [(d,d)]$ for all $d \neq 0 \in D$, as follows:

$$[(a,b)][(1,1)] = [(a,b)] = [(1,1)][(a,b)]$$

This completes the proof that F is a ring.

(c) In fact, F is a commutative ring (because so is D), as shown below:

$$[(a,b)][(x,y)] = [(ax,by)] = [(xa,yb)] = [(x,y)][(a,b)].$$

7. Every nonzero element in F has an inverse:

   Let $(a,b)] \in F$ be nonzero. So, $a \neq 0$ and $(b,a) \in F$. Now, $[(a,b)][(b,a)] = [(ab,ab)] = [(1,1)]$.

This completes the proof that F is a field. The proof is complete. ∎
Now, final question is whether D is a subring of F? Answer is "yes", in the follwing sense.

Lemma 21.4. *The map $i : D \longrightarrow F$ given by $i(a) = [(a,1)] = \frac{a}{1}$ is an injective homomorphism of rings.*

Proof. Clearly $i(a+b) = [(a+b,1)] = [(a,1)]+[(b,1)] = i(a)+i(b)$. Similarly, $i(ab) = i(a)i(b)$. So, i is a ring homomorphism.

Now, we prove i is injective, meaning one to one. In group theory, we learned that it is enough to check that the kernel is zero. So, let $i(a) = [(0,1)]$. That means $[(a,1)] = [(0,1)]$. By definition of the equivalence relation, it follows $a = 0$. The proof is complete. ∎

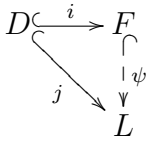
Theorem 21.5. *Let D be an integral domain. Then D can be enlarged to a field F, such that every element is a quotient of two elements of D.*

Proof. Take the injective homomorphism $i : D \longrightarrow F$, as above. Now we identify D by its image $i(D)$, which is an isomorphic "copy" of D. The proof is complete. ∎

21.2 Uniqueness

In fact, this field of quotient is "smallest" in the sense of the following theorem. This theorem can be called an "universal property" of the homomorphism $i : D \longrightarrow F$.

Theorem 21.6. *Let F be the field of quotients of an integral domain D. Let $i : D \longrightarrow F$ denote the "inclusion" homorphism. Let L be a field and $j : D \longrightarrow L$ be an injective homomorphism. Then there is a* **unique injective homomorphism** *$\psi : F \longrightarrow L$ such that $\psi i(a) = j(a)$. If we consider $D \subseteq F$, then $\psi(a) = j(a)$. Diagramatically:*



commutes and $a/b \mapsto (j(a))(j(b))^{-1}$.

Proof. We define $\psi : F \longrightarrow L$ as follows: Let $\frac{a}{b} = [(a, b)] \in F$. Since $b \neq 0$ and j is injective $j(b)$ has an inverse in L. Define

$$\psi\left(\frac{a}{b}\right) = j(a)(j(b))^{-1}$$

To see ψ is well defined, let $[(a, b)] = [(c, d)]$. This means $ad = bc$. So, $j(a)j(d) = j(b)j(c)$. So, $j(a)j(b)^{-1} = j(c)j(d)^{-1}$. So, ψ is well defined.

Now, it is easy it check that

$$\psi(x + y) = \psi(x) + \psi(y) \qquad \psi(xy) = \psi(x)\psi(y).$$

Now to see ψ is injective, let $\psi([(a,b)]) = 0 \in L$. So, $j(a)j(b)^{-1} = 0$. So, $j(a) = 0$. Since j is injective $a = 0$. So, $[(a,b)] = 0 \in F$. So, $\ker(\psi) = \{0\}$ and ψ is injective.

Uniqueness: Suppose there is another homomorphism $\varphi : F \longrightarrow L$ such that $\varphi i(a) = j(a)$ for all $a \in D$. Since φ is a homomorphism,

$$\varphi([(1,b)]) = \varphi([(b,1)]^{-1}) = \varphi([(b,1)])^{-1} = \varphi(i(b)])^{-1} = j(b)^{-1}.$$

So,

$$\begin{aligned}\varphi([(a,b)) &= \varphi([(a,1)][(1,b)]) = \varphi([(a,1)]])\varphi([(1,b)]) \\ &= \varphi(i(b)])^{-1}\varphi(i(b)])^{-1} = j(a)j(b)^{-1} = \psi([(a,b)).\end{aligned}$$

So, $\varphi = \psi$. The proof is complete. ∎

Interpretation: The injecitivity is intepreted as follows:

$$For\ any\ field \quad L, \quad D \subseteq L \Longrightarrow F \subseteq L.$$

Exercise. Let $f : K \longrightarrow L$ be a homomorphism of fields. Prove that f is injective. (Use $f(1) = 1$.)

Definition 21.7. *Suppose D is an integral domain. Any field F, satisfying the universal property, as in theorem 21.6, is called a* **field of quotients** *of D.*

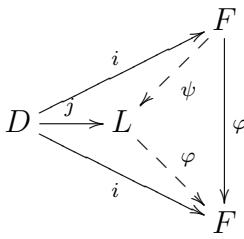
Try to see the analogy with $\mathbb{Z} \subseteq \mathbb{Q}$.

Corollary 21.8. *Any two fields of quotients, of an integral domain D, are isomorphic.*

Proof. Let F, L be two fields of quotients of D. Let us denote the inclusions $i : D \hookrightarrow F$ and $j \hookrightarrow L$. By theorem above there is an injective homomorphism $\psi : F \longrightarrow L$ such the $\psi i(a) = j(a)$ for all $a \in D$.

We will prove that ψ is onto. Since L is also a field of quotients, any element $y \in L$ can be written as $y = j(a)j(b)^{-1}$. So, $\psi(i(a)i(b)^{-1}) = \psi(i(a))\psi(i(b)^{-1}) = j(a)j(b)^{-1} = y$. So, ψ is onto, hence an isomorphism. The proof is complete. ∎

Alternate Proof: with Diagram:



$\varphi\psi = I_F$ *because of uniquenness of such homomorphisms.*

By "existance part" theorem 21.6, ψ, φ exist, so that the diagram commutes. By the "uniqueness part" of theorem 21.6, $\varphi\psi = I_F$. Similarly $\psi\varphi = I_L$. So, ψ is an isomorphism. ■

22 Rings of Polynomials

We formally define polynomials.

Definition 22.1. Suppose R is a ring and x is an indeterminate (a symbol). A **polynomial** $f(x)$ **with coefficients in** R is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots \qquad with \qquad a_i \in R$$

and only finitely many a_i are nonzero.

1. The a_n is called the **coeffient of** x^n **in** $f(x)$.
2. We use the notation $x^n := 1x^n$.
3. Also, we omit the terms $0x^i$. Since only finitely many a_i are nonzero, a polynomial $f(x)$ would look like a finite sum:

   $$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

   perhaps few more terms would be missing, in this expression.
4. Suppose $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is a polynomial, with $a_n \neq 0$. Then, we say $f(x)$ has **degree** n.
5. For $a \in R$ the polynomial

   $$a + 0x + 0x^2 + \cdot \quad ia\ denoted\ by \quad "a" \quad itself.$$

   It is called a **constant polynomial**. A constant polynomial has degree zero.
6. So, one can think of a polynomial as a sequence $a_0, a_1, \ldots, a_n \ldots$ with only finitley many nonzero terms.

7. Suppose

$$f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots \quad and \quad g(x) = b_0 + b_1x + \cdots + b_nx^n + \cdots$$

(a) Define "addition"

$$f(x) + g(x) = c_0 + c_1x + \cdots + c_nx^n + \cdots \quad where \quad c_n = a_n + b_n.$$

(b) Define "multiplication"

$$f(x)g(x) = d_0 + d_1x + \cdots + d_nx^n + \cdots \quad where \quad d_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Theorem 22.2. *Let R be a ring and $R[x]$ be the set of all polynomials in an indeterminate x and coefficients in R.*

1. *Then, $R[x]$ is a ring.*
2. *If R is commutative, so is $R[x]$.*
3. *The ring $R[x]$ is called the* **polynomial ring with coefficients in R.**

Proof. The proof is routine. Verify all the properties of rings. Read it from the textbook. ∎

Question. What are the units of $R[x]$? Assume R is commutative.

Definition 22.3. Define polynomial rings with two variables, as follows.

If y is another indeterminate, then we define $R[x, y] = R[x][y]$ to be called the **polynomial ring in two indeterminate** over R.

Likewise, we define **the polynomial ring $R[x_1, x_2, \ldots, x_n]$ in n indeterminate** $x_1, x_2, \ldots, x_n$.

Lemma 22.4. *The map $R \longrightarrow R[x]$ defined by $a \mapsto a$ is an injective homomorphism. So, we consider $R \subseteq R[x]$ as a subset or "subring".*

Proof. Trivial

Lemma 22.5. *Suppose D is an integral domain. Then, $D[x]$ is an integral domain.*

Proof. Suppose $f(x), g(x) \in R[x]$ and $f(x)g(x) = 0$. We will prove one of them is zero. Assume both are nonzero. Write

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \qquad \textit{and} \qquad f(x) = b_0 + b_1x + \cdots + b_mx^m \qquad \textit{with } a_n \neq 0, b_n \neq 0.$$

Then the coefficient of x^{m+n} (the top degree term) is a_nb_m. Since $f(x)g(x) = 0$, this coefficient $a_nb_m = 0$. Since, D is an integral domain, $a_n = 0$ or $b_n = 0$. Which is a contradiction. So, either $f(x) = 0$ or $g(x) = 0$ The proof is complete. ∎

Remark. Since, $D[x]$ is an integral domain, we can define the field of quotients of $D[x]$, whose elements are written as $f(x)/g(x)$ with $f(x) \neq 0$.

22.1 The Evaluation Homomorphisms

The evaluation homomorphim is my favorite homomorphism.

Theorem 22.6. *Let F be a subring of another ring E. Let $\alpha \in E$. Define the map*

$$\varphi_\alpha : F[x] \longrightarrow E \qquad \textit{by} \quad \varphi_\alpha = f(\alpha).$$

Then, φ_α is a homomorphism.

Proof. For $f(x), g(x) \in R[x]$, we need to show

$$\varphi_\alpha(f(x)+g(x)) = \varphi_\alpha(f(x))+\varphi_\alpha(g(x)) \qquad \textit{and} \quad \varphi_\alpha(f(x)g(x)) = \varphi_\alpha(f(x))\varphi_\alpha(g(x))$$

Or, to prove

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) \qquad \textit{and} \quad (fg)(\alpha) = f(\alpha)g(\alpha)$$

which is obvious. ∎

Example 22.7 (22.6)**.** Let R be any ring. Then, the homomorphism $\varphi_0 : R[x] \longrightarrow R$ is given by

$$\textit{for} \quad f(x) = a_0 + a_1x + \cdots + a_nx^n \quad \textit{we have} \quad \varphi_0(f) = a_0.$$

Example 22.8 (22.7)**.** Consider $\mathbb{Q} \subseteq \mathbb{R}$. Then,

$$\varphi_2 : \mathbb{Q}[x] \longrightarrow \mathbb{R} \quad \textit{is given by} \quad \varphi_2(f) = f(2).$$

Note, $\varphi_2(x^2 - 6) = 0$, $\varphi_2(x - 2) = 0$. The author is trying to amke the point: 2 is zero of these two polynomial.

So, these two polynomials are in $\ker(\varphi_2)$.

Example 22.9 (22.8)**.** Consider $\mathbb{Q} \subseteq \mathbb{C}$. Let $i^2 = -1$. Then,

$$\varphi_i : \mathbb{Q}[x] \longrightarrow \mathbb{R} \quad \textit{is given by} \quad \varphi_i(f) = f(i).$$

Note, $\varphi_i(x^2 + 1) = 0$. The author is trying to amke the point: i is zero of $x^2 + 1$.

So, $x^2 + 1$ in $\ker(\varphi_i)$.

Definition 22.10. *Let F be a subfield of a field E and $\alpha \in E$. Consider the evaluation homomorphism*

$$\varphi_\alpha : F[x] \longrightarrow E \quad \textit{is given by} \quad \varphi_\alpha(f) = f(\alpha).$$

We say α is a **zero** *of f if $f(\alpha) = 0$. That means, if $f \in \ker(\varphi_\alpha)$,*

23 Factorization of Polynomials over a fields

23.1 The Division algorithm

Actually, the divisio algorithm needs a proof.

Theorem 23.1 (Division Algorithm)**.** *Suppose F is a field. Let $g \in F[x]$ and $g \neq 0$ and $degree(g) = m$. Then, given any polynomial $f \in F[x]$, we can write*

$$\exists\ unique \quad r(x), q(x) \in R[x] \quad \ni \quad f(x) = g(x)q(x) + r(x)$$

$$with \quad r(x) = 0 \quad or \quad degree(r(x)) < m.$$

Proof. (**Existance**): Write

$$S = \{f(x) - g(x)q(x) : q(x) \in R[x]\}$$

If $0 \in S$ then $\exists\ q(x) \in R[x] \ni \quad f(x) = g(x)q(x)$. So, the algorithm is valid with $r(x) = 0$.

Now suppose $0 \notin S$. Let

$$d = \min\{degree(\rho) : \rho \in S\}$$

Pick

$$r(x) = f(x) - g(x)q(x) \in S \ \ni \quad degree(r(x)) = d.$$

I claim, that $d < m$. If not let $d \geq m$. Write

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad r(x) = c_0 + c_1x + \cdots + c_dx^d$$

with $b_m \neq 0, c_d \neq 0$. Now,

$$\rho(x) = r(x) - g(x)\frac{c_dx^{d-m}}{b_m} \quad has\ degree \quad \leq d - 1.$$

Also,

$$\rho(x) = r(x) - \frac{c_dx^{d-m}}{b_m}g(x) = f(x) - g(x)\left(q(x) + \frac{c_dx^{d-m}}{b_m}\right) \in S.$$

Since $0 \notin S$, $\rho(x) \neq 0$. The minimality of d is contradicted, because $degree(\rho(x)) \leq d-1$. So, it is established $degree(r(x)) \leq m-1$. So, we have $f(x) = g(x)q(x)+r(x)$ with $degree(r(x)) \leq d-1$. So, the algorithm holds.

Now, we prove uniqueness. Suppose

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

$$where \quad r_i(x) = 0 \quad or \quad degree(r_i) \leq m-1.$$

Subtracting, we have

$$r_1(x) - r_2(x) = g(x)(q_1(x) - q_2(x))$$

Since, $degree(r_1(x) - r_2(x)) \leq m-1 < m = degree(g)$, we have $q_1(x) - q_2(x) = 0$. Hence $r_1(x) - r_2(x) = 0$. So, $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. So, uniqueness is established. The proof is complete. ∎

Theorem 23.2 (Generalized Division Algorithm)**.** *Let R be a commutative ring. Let $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in R[x]$.* (Note coefficient of x^m in G is 1. Such a polinomial is called a **monic polynomial.**) *Then, given any polynomial $f \in F[x]$, we can write*

$$\exists\ unique \quad r(x), q(x) \in R[x] \quad \ni \quad f(x) = g(x)q(x) + r(x)$$

$$with \quad r(x) = 0 \quad or \quad degree(r(x)) < m.$$

Proof. Exercise

Long Division: The long division method of dividing applies in all these cases.

Example 23.3 (23.2)**.** in $\mathbb{Z}_5[x]$ divide a give $f(x)$ by $g(x) = x^2 - 2x + 3$, by **long division**. **Please read it.**

Objective of this section is to write any polynomial $f(x)$ over a field, as product of "irreducible polynomials". Simplest among the irreducible polynomials are the linear polynomial $x - a$.

Corollary 23.4 (Factor Theorem)**.** Let F be field and $a \in F$ and $f(x) \in F[x]$. Then, a is a zero of f if and only if $x - a$ is a factor of $f(x)$.

Proof. ($\Leftarrow$): Suppose $x - a$ is a factor of $f(x)$. So, $f(x) = (x - a)q(x)$ for some $q(x) \in F[x]$. So, $f(a) =$ and hence a is a zero of $f(x)$.

($\Rightarrow$): Now suppose a is a zero of f, which means $f(a) = 0$. Now divide $f(x)$ by $x - a$, we have

$$f(x) = (x - a)q(x) + r(x)$$

where $r(x) = 0$ or $degree(r(x) = 0$ (i.e. $r(x) = r \in F)$. Substituting $a = 0$ we have $r = r(0) = 0$. So, $f(x) = (x - a)q(x)$. The proof is complete. ∎

Example 23.5 (23.4)**.** in $\mathbb{Z}_5[x]$ use **long division** and apply the corollary (23.4). **Please read it.**

Corollary 23.6. *Let F be a field and $f(x) \in F[x]$ be a nonzero polynomial of degree n. Then $f(x)$ can have at most n zeros.*

Proof. Suppose a_1 is a zero of $f(x)$. Then,

$$f(x) = (x - a_1)q_1(x)$$

for some polynomial $q_1(x)$ of degree $n - 1$. Now, if a_2 is a zero of q_1 then $x - a_2$ is a factor of q_2, which gives

$$f(x) = (x - a_1)(x - a_2)q_2(x) \quad where \quad degree(q - 2) = n - 2.$$

Repeating this process, we can write

$$f(x) = (x - a_1)(x - a_2)\cdots(x - a_r)q_r(x) \quad where \quad degree(q - 2) = n - r.$$

and $q_r(x)$ has no zero in F. Since, degree of f is n, there can be at most n such linear factors. Also, $a_1, \ldots, a_r$ are theonlt zeros of f in F, because if $b \neq a_i$ then $f(b) = (b - a_1)(b - a_2)\cdots(b - a_r)q_r(b) \neq 0$. Hence $a_1, \ldots, a_r$ are the only zeros of $f9x)$ and $r \leq n$. The proof is complete. ∎

Corollary 23.7. *Let F be a field and G be a FINITE subgroup of the multiplicative group F^*. Then G is cyclic.*

Proof. It is an application of theorem 11.12. We omit the proof. ∎

23.2 Irreducible Polynomials

As I mentioned above simplest of all the irreducible polynomials are linear polynomials $x - a$.

Definition 23.8. *Let F be a field and $f(x) \in F[x]$ be nonconstant polynomial. We say that $f(x)$ is* **irreducible over** *F or is an* **irreducible polynomial in** *$F[x]$ if*

$$[f(x) = g(x)h(x) \quad \textit{with } g, h \in F[x]] \quad \Longrightarrow \quad [f \in F \textit{ or } g \in F].$$

A nonconstant polynomial $f(x) \in F[x]$ is said to be **reducible***, if it is not irreducible.*

Remarks. Here are some comments:

1. We restate the definition. A nonconstant polynomial f is irreducible, if it has no nontrivial factorization $f(x) = g(x)h(x)$. For example, $\forall\, a \in F,\ a \neq 0$ (i.e. unit in $F[x]$), there is always a trivial factorization $f(x) = a(a^{-1}f(x))$.
2. All linear polynomials $ax + b$, with $a \neq 0$, are irreducible.
3. Suppose F is a subfiled of a field E. It is possible that a polynomial $f(x) \in F[x]$ is irreducible over F, but not over E. Some examples follows.

Example 23.9. Here are some examples.

1. **(23.8)** $f = x^2 - 2 \in \mathbb{Q}[x]$. Although $f = x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, it is reducible in $\mathbb{R}[x]$.
2. $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$, it is reducible in $\mathbb{C}[x]$. Reducible polynomials in $\mathbb{R}[x]$ are linear or quadratic (why?). In fact, all irreducible polynomials in $\mathbb{C}[x]$ are linear(why?).

Example 23.10 (23.9)**.** The polynomial $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]$ is irreducible in $\mathbb{Z}_5[x]$.

Proof. If $f(x)$ is reducible, then $f(x) = g(x)h(x)$, both $g(x)$ and $h(x)$ are nonconstant. So, one of them has degree 2 and other one has degree one. Suppose $g(x) = ax + b$ is the linear factor. Then, $-ba^{-1}$ is a zero of g and hence of f. So, we conclude that, if f is irreducible in $\mathbb{Z}_5[x]$, then it has a zero in $\mathbb{Z}_5$. But

$$f(0) = 2, f(1) = 1, f(2) = 1, f(3) = 3, f(4) = 3.$$

So, f is irreducible. The proof is complete. ■

Theorem 23.11. *Let F be a field and $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Then, $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Proof. ($\Leftarrow$): Suppose $a \in F$ is a zero of $f(x)$. Then $(x - a)$ is a factor of f. So, $f(x) = (x - a)h(x)$ is a nontrivial factorization of f. So, f is reducible.

($\Rightarrow$): Suppose F is reducible. Let $f(x) = g(x)h(x)$ be a nontrivial factoriztion, with $g, h \in F[x]$. Since f has degree 2 or three, g or h has degree one. Assume $g(x) = (ax + b)$ is linear, with $a \neq 0$. So, $f(x) = (ax + b)h(x)$. So, $-ba^{-1}$ is a zero of f in F. The proof is complete. ■.

23.3 Irreducibility in $\mathbb{Q}[x]$

I will add some material from the book of Herstein.

Definition 23.12. Suppose $f(x) \in \mathbb{Z}[x]$. Write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}$.

1. Define **content** of f as $content(f) = \gcd(a_0, a_1, \ldots, a_n)$.
2. We say that f is **primitive**, if $content(f) = 1$.

Lemma 23.13. *Let $f(x), g(x) \in \mathbb{Z}[x]$ be two premitive polynomials. Then, $f(x)g(x)$ is also a premitive polynomial.*

Proof. Write

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad and \quad g(x) = b_0 + b_1x + \cdots + b_mx^m$$

Suppose p is a prime number. We will show p does not divide some coefficient of $f(x)g(x)$. Since f is primitive p does not divide some coefficient of f. Let a_j be the first one:

$$p|a_0, p|a_1, \ldots, p|a_{j-1}, p \not| a_j.$$

Similarly, there is a k such that

$$p|b_0, p|b_1, \ldots, p|b_{k-1}, p \not| b_k.$$

Now, coefficient c_{j+k} of x^{j+k} in $f(x)g(x)$ is give by $c_{j+k} =$

$$a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{j+k})$$

Now, $p \not| a_jb_k$ and all the other terms are divisibe by p. So, $p \not| c_{j+k}$. The proof is complete.

Alternate Proof. I will give a different proof, in class, using "modulo p" calcualtions and the product of two monic polynomials is monic. ∎

Theorem 23.14 (23.11)**.** *Suppose $f(x) \in \mathbb{Z}[x]$. Suppose*

$$f(x) = g(x)h(x) \quad with \quad g, h \in \mathbb{Q}[x], degree(g) = r, degree(h) = s.$$

Then,

$$f(x) = \lambda(x)\mu(x) \quad with \quad \lambda, \mu \in \mathbb{Z}[x], degree(\lambda) = r, degree(\mu) = s.$$

Proof. Let $c = content(f)$. So, $f(x) = c\varphi(x)$ and $\varphi(x)$ is premitive. We can write $g(x) = \frac{u\lambda(x)}{v}, h(x) = \frac{u'\mu(x)}{v'}$, where $u, u', v, v' \in \mathbb{Z}$ and λ, μ are premitive polynomials in $\mathbb{Z}[x]$. Writing $\frac{a}{b} = \frac{uu'}{vv'}$, the equation $f(x) = g(x)h(x)$ reduces to

$$f(x) = c\varphi(x) = \frac{a}{b}\lambda(x)\mu(x). \quad hence \quad cb\varphi(x) = a\lambda(x)\mu(x)$$

where φ, λ, μ are primitive. So, $\lambda(x)\mu(x)$ is also premitive. So, the content of the left side is cb and content of the right side is a. So, $a = cb$ or $\frac{a}{b} = c$. So,we get

$$f(x) = (c\lambda(x))\mu(x).$$

The proof is complete. ∎

Corollary 23.15. *Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial in $\mathbb{Z}[x]$ with $a_0 \neq 0$.* (**monic** means the coefficient of the to degree term is 1)*. Then,*

$$f(a) = 0 \text{ for some } a \in \mathbb{Q} \implies f(m) = 0 \text{ for some } m \in \mathbb{Z} \text{ and } n|a_0.$$

Proof. Suppose $a \in \mathbb{Q}$ is a zero of f. Then $f(x) = (x - a)g(x)$, with $g(x) \in \mathbb{Q}[x]$. By (23.14), $f(x) = (cx - m)h(x)$ for some $h \in \mathbb{Z}[x]$ and $c, m \in \mathbb{Z}$ with $c \neq 0$. Write $h(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ with $b_i \in \mathbb{Z}$. The equation $f(x) = (cx - m)h(x)$ can be written as

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (cx - m)(b_{n-1}x^{n-1} + \cdots + b_1x + b_0).$$

Comparing the coefficient of x^n, we have $cb_{n-1} = 1$. So, $c = \pm 1$. We can assume $c = 1$. So, m is a zero of f. Comparing the constant terms $a_0 = mb_0$. So, $b_0 = a_0/m$. The proof is complete. ∎

Example 23.16 (23.14)**.**

$$We\ prove \quad f(x) = x^4 - 2x^2 + 8x + 1 \quad is \quad irreducible \quad \mathbb{Q}[x].$$

Proof. Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$. Then $f(x) = g(x)h(x)$, where $g, h \in \mathbb{Q}[x]$, both non-constant. We deal with two cases.

1. Suppose g or h is linear. Then, $f(x)$ has a zero in $\mathbb{Q}$. By corollary (23.15), $f(x)$ has a zero m in $\mathbb{Z}$ and m divides the constant term of f, which is 1. So, $m = \pm 1$. But $f(1) = 8, f(-1) = -8$, which is impossible. So, neither g nor h is linear.

2. Now assume both g, h are quadratic. By (23.14), f factors into two quadratics in $\mathbb{Z}[x]$. Write

   $$f(x) = x^4 - 2x^2 + 8x + 1 = (a_0x^2 + ax + b)(b_0x^2 + cx + d) \quad with \quad a_0, b_0, a, b, c, d \in \mathbb{Z}.$$

   Comparing coefficient of x^4, we have $1 = a_0b_0$. So, $a_0 = b_0 = 1$ or $a_0 = b_0 = -1$. However, if $a_0 = b_0 = -1$, we can change sigms of a, b, c, d and assume $a_0 = b_0 = 1$. So, we rewrite the above equations as:

   $$f(x) = x^4 - 2x^2 + 8x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

   Comparing the coefficients of x^3, x^2, x, x^0 we have

   $$a + c = 0, b + d + ac = -2, ad + bc = 8, bd = 1.$$

   Fram, $bd = 1$ we get

   $$b = d = 1 \quad or \quad b = d = -1$$

   Substituting in $ad + bc = 8$ we get

   $$a + c = 8 \quad or \quad a + c = -8. \quad This\ contradicits \quad a + c = 0.$$

   So, f cannot have any quadratic factors.

Therfore, f is irreducible in $\mathbb{Q}[x]$. The proof is complete. ∎

Theorem 23.17 (Eisenstein Criterion)**.** *Let $p \in \mathbb{Z}$ be a prime. Suppose $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, such that*

$$p|a_0, p|a_1, \ldots, p|a_{n-1}, \quad but \quad p \not| a_n, \quad and \quad p^2 \not| a_0.$$

Then, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. By (23.14) we have to show, that $f(x)$ does not factor into polynomials of of lower degrees in $\mathbb{Z}[x]$. Suppose,

$$f(x) = (b_rx^r + \cdots + b_0)(c_sx^s + \cdots + c_0) \quad with \ b_r \neq 0, c_s \neq 0 \ and \ r < n, s < n.$$

1. We have $a_0 = b_0c_0$. Since $p^2 \not| a_0$ not both b_0, c_0 are divisible by p. Assume $p \not| b_0$. Since $p|a_0$, $p|c_0$.

2. Since, $p \not| a_n$, we have $p \not| b_r, p \not| c_s$.

3. We have $p|c_0, p \not| c_s$. Let $1 \leq m \leq s$ be such that

$$p|c_0, p|c_1, \cdots, p|c_{m-1}, \quad but \quad p \not| c_m.$$

4. Comparing coefficient of x^m we have

$$a_m = b_0c_m + b_1c_{m-1} + \cdots + \begin{cases} b_mc_0 & if\ r \geq m \\ b_rc_{m-r} & if\ r < m. \end{cases}$$

The first term is not divisible by p and other terms are divisible by p. So, $p \not| a_m$. So, $m = s = n$, which is impossible. So, above factorization is not possible.The proof is complete. ∎

Example 23.18 (23.16)**.** Use Eisenstein Criterion, to prove that $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ is irreducible in $\mathbb{Q}[x]$.

Proof. take $p = 3$. ∎

Corollary 23.19. *The polynomial* $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *is irreducible over* $\mathbb{Q}$ *for any prime* p.

Proof. It is enough to prove that $\Phi_p(x+1)$ is irreducible (why?). First note

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

So,

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{\left(x^p + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-1} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} x + 1\right) - 1}{x}$$

$$= x^{p-1} + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-2} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix}$$

By Eisenstein Criterion $\Phi_p(x+1)$ is irreducible hence so is $\Phi_p(x)$. The proof is complete. ∎

23.4 Unique Factorization

We use the language "g divides f" before. The textbook gives a definition:

Definition 23.20. For two elements f, g in a commutative ring R, we say that g **divides** f, if $f = gq$ for some $q \in R$. In this case, we also write $g|f$.

Theorem 23.21. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Suppose $r(x), s(x) \in F[x]$, then*

$$p|r(x)s(x) \quad \Longrightarrow \quad either \quad p(x)|r(x) \quad or \quad p(x)|s(x).$$

Proof. Delayed untill §27.

Corollary 23.22. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial and $r_i(x) \in F[x]$.*

$$If \quad p(x)|(r_1(x)r_n(x)\cdots r_n(x)) \quad then \quad p(x)|r_i(x) \quad for\ some \quad i.$$

Proof. This is proved by induction. If $n = 2$ then the assertion holds for by the theorem above. For the inductive step, assume the assertion holds for product of $n-1$ polynomials. Now suppose $p(x)|(r_1(x)r_n(x)\cdots r_n(x))$. We can rewrite it as $p(x)|[r_1(x)r_n(x)\cdots r_{n-1}(x)]r_n(x)$. Since it is true for $n = 2$, we have

$$p(x)|(r_1(x)r_n(x)\cdots r_{n-1}(x)) \quad or \quad p(x)|r_n(x).$$

In case, $p(x)|(r_1(x)r_n(x)\cdots r_{n-1}(x))$ then by induction hypothesis $p(x)|r_i(x)$ for some $1 \leq i \leq n-1$. The proof is complete. ∎

Lemma 23.23. *Suppose $p(x) \in F[x]$ is an irreducible polynomial. Let $u \neq 0 \in F$. Then $up(x)$ is irreducible.*

Proof. Suppose $up(x) = g(x)h(x)$. Then $p(x) = (u^{-1}g(x))h(x)$. Since p is irreducible, either $u^{-1}g(x) \in F$ or $h(x) \in F$. This implies, either $g(x) \in F$ or $h(x) \in F$. So, up is irreducible. The proof is complete. ∎

Lemma 23.24. *Suppose $p(x), q(x) \in F[x]$ ar two irreducible polynomials. If $p|q$ then $p(x) = uq(x)$ for some unit $u \in F$.*

Proof. Suppose $p(x) = u(x)q(x)$. Since p is irreducible, $u(x) \in F$. ∎

Theorem 23.25. *Let F be a field and $f(x) \in F[x]$ be a nonconstant polynomial. Then, f can be written as the product of irreducible polynomials. This factorization is unique, except of the order and for units in F (same as units in $F[x]$).* (See the proof for better understanding of the uniqueness statement.)

Proof. Suppose $f(x)$ is a nonconstant polynomial. First, we prove that $f(x)$ can be written as product of irreducible polynomials. We use induction of degree of f to prove this. If $degree(f) = 1$, then F is irreducble and the assertion holds.

Now assume $degree(f) = d \geq 2$. If f is irreducible then the assertion holds. If f is not irreducible then $f(x) = g(x)h(x)$ where both $g(x), h(x)$ are nonconstant. So, $degree(g(x)) < degree(f(x))$ and $degree(h(x)) < degree(f(x))$. So, by induction, both g and h are product of irreducible polynomial. So, it is established that $f(x)$ is product of irreducible polynomial.

Now, we prove that such factoriztions are unique. Suppose

$$f = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad where \quad p_i, q_i \in F[x] \quad irreducible.$$

We will prove $r = s$ and we can reorder (label) q_i, so that $p_i = u_i q_i$ for some units $u_i \in F$. We assume $s \geq r$.

Since p_1 divides $q_1 q_2 \cdots q_s$. By (23.22), $p_1 | q_i$ for some $i = 1, \ldots, s$. By re-labeling, we assume $p_1 | q_1$. So, $q_1(x) = u_1 p_1(x)$ for some unit $u \in F$. So, we have

$$p_1(p_2 p_3 \cdots p_r) = u_1 p_1(q_2 q_3 \cdots q_s). \quad So, \quad p_2 p_3 \cdots p_r = u_1 q_2 q_3 \cdots q_s.$$

By similar argument (or by induction)

$$q_2 = u_2 p_2, \ldots, q_r = u_r p_r \quad for\ some\ units \quad u_i \in F.$$

So, we have

$$p_1 p_2 \cdots p_r = (u_1 u_2 \ldots u_r)(p_1 p_2 \cdots p_r)(q_{r+1} \cdots q_s). \qquad Hence \quad 1 = (u_1 u_2 \ldots u_r)(q_{r+1} \cdots q_s).$$

So, $q_{r+1}, \ldots, q_s$ are units in F. This is impossible because q_i are irreducible. So, $r = s$. The proof is complete. ∎

Remark. Compare this with factorization theorems in $\mathbb{Z}$.

24 Noncommutative Examples

We did not give too many examples of noncommutative rings and noncommutative groups. We will not work with noncommutative situation very much. In this section we give some example.

Example 24.1. Most commonly encountered non-commutative ring are the ring $M_n(R)$ of all square matrices of order n with entries in a commutative ring R. This includes,

$$M_n(\mathbb{Z}), M_n(\mathbb{Z}_n), M_n(\mathbb{Q}), M_n(\mathbb{R}), M_n(\mathbb{C})$$

and $M_n(F)$ where F is any field.

Example 24.2. Let F be a field and V be a vector space over a field F with $\dim V = n$. In Math 790 (or 290), we have seen that, there is a one to one correspondance between the linear transforamtion $f : V \longrightarrow V$ and elements in $M_n(F)$.

Let $End_F(V)$ denotes the set of all linear transforamtion $f : V \longrightarrow V$. Then $End_F(V)$ is a ring under addition and composition as the multiplication.

In fact, $End_F(V)$ is a noncommutative ring. It follows from the fact that $M_n(F)$ is noncommutative, if $n \geq 2$.

Likewise, we have the following.

Example 24.3. Let G be ab abelian group. Let $End(G)$ denote the set of all group homomorphism $f : G \longrightarrow G$. Then, $End(G)$ a ring under addition and composition as the multiplication.

In fact, $End(G)$ is a noncommutative ring.

24.1 Group Rings

Let $G = \{g_i : i \in I\}$ be any group, written multiplicatively and R be any commutative ring.

1. Let $R(G)$ denote the set of all formal sums

$$\sum_{i \in I} a_i g_i \qquad where \qquad a_i \in R$$

   and only finitely many a_i are nonzero.

2. Define addition:

$$\sum_{i \in I} a_i g_i + \sum_{i \in I} b_i g_i = \sum_{i \in I} (a_i + b_i) g_i$$

3. Define multiplication

$$\left(\sum_{i \in I} a_i g_i \right) \left(\sum_{i \in I} b_i g_i \right) = \sum_{i \in I} \sum_{g_j g_k = g_i} (a_j b_k)\, g_i$$

4. Then, $R(G)$ **is ring.** If G is nnoabelian, then $R(G)$ is noncommutative.

25 Ordered Rings and Fields

We know that the field of real numbers $\mathbb{R}$ has an order realtion $\leq$. In that spirit we define ordered rings as follows.

Definition 25.1. *An* **ordered ring** *R is ring R together with a nonempty subset $P \subseteq R$ satisfying the following two properties:*

1. $\forall\ a, b \in P \quad a + b \in P \quad and \quad ab \in P$
2. *For each $a \in R$, one and only one of the following holds:*

$$a \in P, \quad a = 0, \quad -a \in P.$$

The elements in P are called **positive elements**.

Theorem 25.2. Let R be an ordered ring, with the set P of positive elements. Let $<$. read "less than" be the relation defined by

$$a < b \quad if \quad b - a \in P$$

Such a relation has the following properties $\forall\ a.b.c \in R$:

1. (**Tricotomy**): One and only one of the following holds:

$$a < b, \quad a = b, \quad b < a.$$

2. (**Transitivity**): $a < b < c \quad \Longrightarrow \quad a < c.$
3. (**Isotonicity**):
   (a) $b < c \quad \Longrightarrow \quad a + b < a + c$
   (b) $b < c \quad and \quad 0 < a \quad \Longrightarrow \quad ab < ac \ and \ ba < ca.$