Part 2: Rings

12 Introduction to Rings

12.1 Motivation and Definition

Definition Ring

> A ring R os a set with two binary operations, addtion and multiplication, such that for all a, b, c in R:
>
> 1. $a + b = b + a$.
> 2. $(a + b) + c = a + (b + c)$.
> 3. There is an additive identity 0. This is , there is an element 0 in R such that $a + 0 = a$ for all a in R.
> 4. There is an element $-a$ in R such that $a + (-a) = 0$.
> 5. $a(bc) = (ab)c$.
> 6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

- A ring is an Abelian group under addition, also having an *associative* multiplication that is left and right *distributive* over addition.
- A ring need not have an identity under multiplication (**unity**). a is a **unit** if a^{-1} exists.

12.2 Examples of Rings

- $\mathbb{Z}$, $\mathbb{Z}_n$, $n\mathbb{Z}$, $\mathbb{Z}[x]$, $M_n(\mathbb{Z})$
- $(f + g)(a) = f(a) + g(a)$, $(fg) = f(a)g(a)$.
- Direct sum: $R_1 \oplus R_2 \oplus \cdots \oplus R_n$.

12.3 Properties of Rings

Theorem 12.1 Rules of Multiplication

> Let a, b and c belong to a ring R. Then
>
> 1. $a0 = 0a = 0$.
> 2. $a(-b) = (-a)b = -(ab)$.
> 3. $(-a)(-b) = ab$.
> 4. $a(b - c) = ab - ac$, $(b - c)a = ba - ca$.
>
>   Futhermore, if R has a unity element 1, then
> 5. $(-1)a = -a$.
> 6. $(-1)(-1) = 1$.

Theorem 12.2 Uniqueness of the Unity and Inverses

> If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

- The ring need not have mutliplicative cancellation: $a \neq 0,\ ab = ac \quad \nRightarrow \quad b = c$.
- The ring need not have a mutliplicative identity: $a^2 = a \quad \nRightarrow \quad a = 0$ or 1.

12.4 Subrings

Definition Subring

> A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

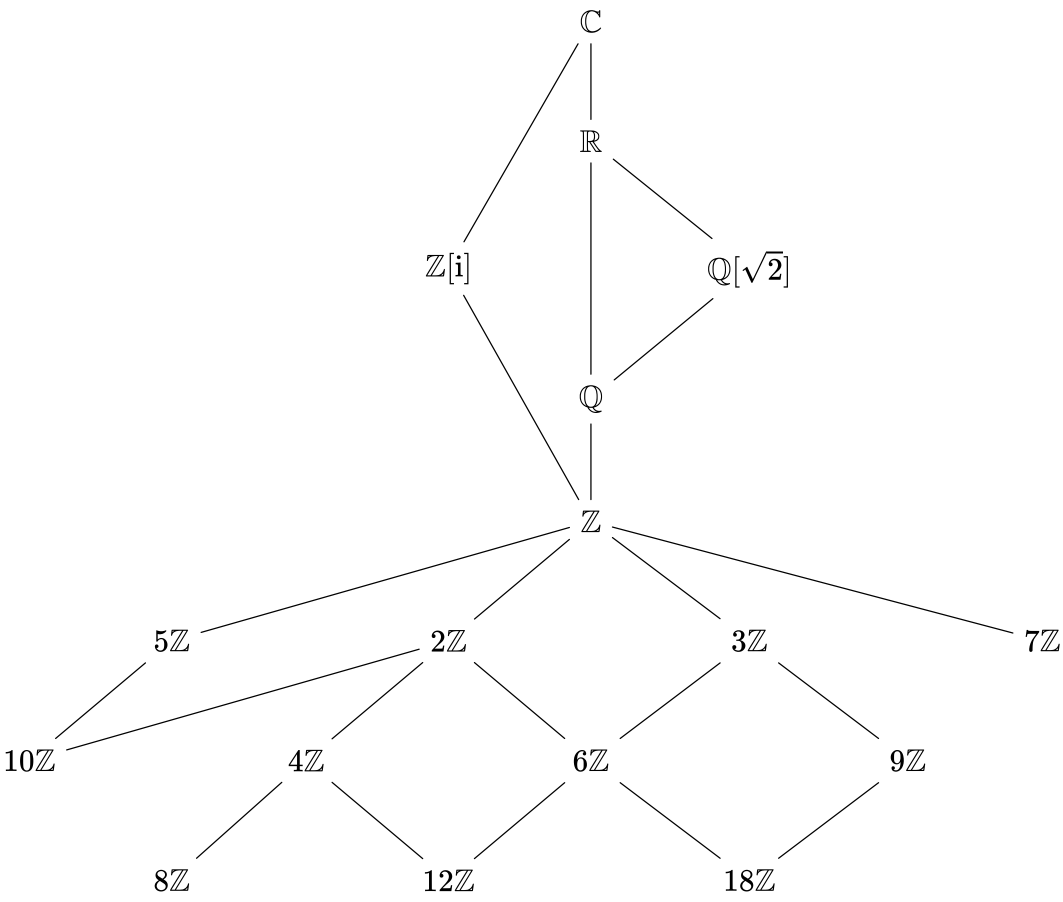
- The subring $2\mathbb{Z}_{10}$ of $\mathbb{Z}_{10}$, has a unity 6 and every nonzero element is a unit of $2\mathbb{Z}_{10}$, but none of these elements is a unit in $\mathbb{Z}_{10}$.

- The intersection of any collection of subring of a ring R is a subring of R.

Theorem 12.3 Subring Test

> A nonempty subset S of a ring R is a subring if S is closed under subtraction and mutliplication. In symbols, $\forall a, b \in S$,
>
> $$a - b,\ ab \in S.$$

Subring lattice diagram



12.5 Exercises

1. A ring is commutative if it has the property that $ab = ca\,(a \neq 0)$ implies $b = c$. (Both outer cancellation and inner cancellation imply commutativity.)
2. Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that $b \mid c \Leftrightarrow ab \mid c$.
3. Let $a, b \in R$, $m, n \in \mathbb{Z}$, then $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$, and $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.
4. A ring that is cyclic under addition is commutative.
5. The center of a ring is a subring.
6. Let $U(R)$ denote the set of units of a commutative ring R, then $U(R)$ is a group under the multiplication of R.
7. Suppose that a and b belong to a commutative ring R with unity. If a is a unit of R and $b^2 = 0$, show that $a + b$ is a unit of R. ($(a + b)(a^{-1} - a^{-2}b) = 1$)
8. **Nilpotent**: $x^n = 0\,(n > 1)$.
    1. Let a be a nilpotent, prove that $1 - a$ has a multiplicative inverse.

2. The nilpotent elements of a commutative ring form a subring.
3. $\mathbb{Z}_n$ has a nonzero nilpotent element if and only if n is divisible by the square of some prime. (Hint: $n = p^2 m,\ (pm)^2 = 0$)

9. **Idempotent**: $x^n = x\ (n > 1)$.
   1. $x = x^{1+m(n-1)}$.
   2. $\exists m \in \mathbb{N}^+,\ x^m = 0 \quad \Rightarrow \quad x = 0$.
   3. $ab = 0 \quad \Rightarrow \quad ba = 0$. (It's not true in $M_n(\mathbb{R})$.)
   4. $2x = 2^n x^n = 2^n x \quad \Rightarrow \quad (2^n - 2)x = 0$.
   5. If a and b are idempotent, then $a^{n_1} + k_1 b^{n_2} + k_2 a^{n_3} b^{n_4}$ is idempotent.
10. **Boolean ring**: $x^2 = x$ for all x in R.
    1. $-x = (-x)^2 = x \quad \Rightarrow \quad 2x = 0$.
    2. Boolean ring is commutative:
       $a + b = (a+b)^2 = a + ab + ba + b \quad \Rightarrow \quad ab = -ba = ba$.
11. There is no integer $n > 1$ such that $a^n = a$ for all a in $\mathbb{Z}_m$ when m is divisible by the square of some prime.
12. Let R be a commutative ring with more than one element. Prove that if for every nonzero element a of R we have $aR = R$, then R has a unity and every nonzero element has an inverse.

12.6 Bibliography of I.N.Herstein

13 Integral Domains

13.1 Definition and Examples

Definition Zero-Divisors

> A zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition Integral Domain

> An integral domain is a commutative ring with unity and no zero-divisors.

- Integral domain: $\mathbb{Z},\ \mathbb{Z}[x],\ \mathbb{Z}[\sqrt{2}],\ \mathbb{Z}_p$.
- Not an integral domain: $M_2(\mathbb{Z}),\ \mathbb{Z} \oplus \mathbb{Z}$.

Theorem 13.1 Cancellation

> Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

13.2 Fields

Definition Field

> A field is a commutative ring with unity in which every nonzero element is a unit.

- Every field is an integral domain.
- A field is an algebraic system that is closed under addition, subtraction, multiplication and division (except by 0).

Theorem 13.2 ⭐

> A finite integral domain is a field.

Corollary $\mathbb{Z}_p$ Is a Field

> For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p is a field.

- Field: $\mathbb{Z}_3[i]$, $\mathbb{Q}[\sqrt{2}]$.
- Not a field: $\mathbb{Z}_5[\mathrm{i}]$.

Theorem Subfield Test

> Let F be a field and let K be a subset of F with at least two elements. Then K is a subfield of F if and only if $\forall a, b\,(b \neq 0) \in K$
>
> $$a - b,\ ab^{-1} \in K.$$

13.3 Characteristic of a Ring

Definition Characteristic of a Ring

> The **characteristic** of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\operatorname{char} R$.

Review that the exponent of a group G is the positive integer n such that $x^n = e$ for all x in G.

- $\operatorname{char}\mathbb{Z} = 0,\ \operatorname{char}\mathbb{Z}_n = n,\ \operatorname{char}\mathbb{Z}_2[x] = 2.$
- $\operatorname{char} R$ divides $|R|$, and a finite ring must have a nonzero characteristic.

Theorem 13.3 Characteristic of a Ring with Unity

> Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Theorem 13.4 Characteristic of an Integral Domain

> The characteristic of an integral domain is 0 or prime.

Ring	Unity	Commutative	Integral Domain	Field	Characteristic
$\mathbb{Z}$	1	Yes	Yes	No	0
$\mathbb{Z}_n$	1	Yes	No	No	n
$\mathbb{Z}_p$	1	Yes	Yes	Yes	p
$\mathbb{Z}[x]$	$f(x) = 1$	Yes	Yes	No	0
$n\mathbb{Z}$	None	Yes	No	No	0
$M_n(\mathbb{Z})$	E_n	No	No	No	0
$M_2(2\mathbb{Z})$	None	No	No	No	0
$\mathbb{Z}[\mathrm{i}]$	1	Yes	Yes	No	0
$\mathbb{Z}_3[\mathrm{i}]$	1	Yes	Yes	Yes	3
$\mathbb{Z}_5[\mathrm{i}]$	1	Yes	No	No	5

Ring	Unity	Commutative	Integral Domain	Field	Characteristic
$\mathbb{Z}[\sqrt{2}]$	1	Yes	Yes	No	0
$\mathbb{Q}[\sqrt{2}]$	1	Yes	Yes	Yes	0
$\mathbb{Z}\oplus\mathbb{Z}$	$(1,1)$	Yes	No	No	0

13.4 Exercises

1. For a nonzero element a in $\mathbb{Z}_n$, if $\gcd(a,n)=1$, then a is a unit, else a is a zero-divisor.
2. Every nonzero element of a finite commutative ring with unity is either a zero-divisor or a unit.

   Hint: Let $s\in R$, $S=\{sr\mid r\in R\}$.
3. If d is an integer, then $\mathbb{Z}[\sqrt{d}]=\left\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\right\}$ is an integral domain, and $\mathbb{Q}[\sqrt{d}]$ is a field. $\mathbb{Z}_p[\sqrt{k}]=\left\{a+b\sqrt{k}\mid a,b\in\mathbb{Z}_p\right\}$ is a field if and only if $a^2\neq b^2k$.
4. Let R be a ring with unity. If the product of any pair of nonzero elements of R is nonzero, then $ab=1\Leftrightarrow ba=1$.
5. $P=\{n\cdot 1\mid n\in\mathbb{Z}\}$ is a **subdomain** of any integral domain D with unity 1, and $|P|=\operatorname{char} D$ (a prime or ∞).
6. If a field F has order p^n, then $\operatorname{char} F=p$.
7. Show that a finite commutative ring with no zero-divisors and at least two elements has a unity.
8. Suppose a and b belong to a commutative ring and ab is a zero-divisor, then a or b is a zero-divisor.
9. If R is a commutative ring without zero-divisors, then
   1. All the nonzero elements of R have the same additive order.
   2. The characteristic of R is 0 or prime.
10. Any finite field has order p^n.
11. Let $x_1,x_2,\cdots,x_n$ belong to a commutative ring R with prime characteristic p, then
    1. $(x_1+x_2+\cdots+x_n)^{p^m}=x_1^{p^m}+x_2^{p^m}+\cdots+x_1^{p^m}$.
    2. If $a\in R$ is a nilpotent of degree k, then $(1+a)^{p^k}=1$.
    3. $K=\{x\in R\mid x^p=x\}$ is a subring of R.
12. Let $\mathbb{F}$ be a finite field with n elements, prove that $x^{n-1}=1$ for all nonzero x in $\mathbb{F}$.
13. Let S be a subring of a ring R and suppose that u_S is a unity in S and u_R is a unity in R and $u_S\neq u_R$, then $u_Su_R=u_Su_S\Rightarrow u_S(u_R-u_S)=0$.

14 Ideals and Factor Rings

14.1 Ideals

Definition Ideal

> A subring A of a ring R is called a (two-sided) **ideal** of R if $\forall r\in R$, $\forall a\in A$, $ar, ra\in A$.

- In other words, $\forall r \in R,\ rA \subseteq A,\ Ar \subseteq A$.
- If A is an ideal of a ring R and 1 belongs to A, then $A = R$ since $r \cdot 1 = r \in A$.
  - If an ideal I of a ring R contains a unit, then $I = R$.
  - The only ideals of a field $\mathbb{F}$ are $\{0\}$ and $\mathbb{F}$ itself and viceversa.
- The interesction of any set of ideals of a ring is an ideal.
- The sum of ideals $A + B = \{a + b \mid a \in A,\ b \in B\}$ is an ideal.
  - $\langle m, n\rangle = \langle m\rangle + \langle n\rangle = \langle \gcd(m, n)\rangle$.
- The product of ideals $AB = \{a_1b_1 + a_2b_2 + \cdots a_nb_n \mid a_i \in A,\ b_i \in B,\ n \in \mathbb{N}^+\}$ is an ideal.
  - $\langle m\rangle \langle n\rangle = \langle mn\rangle$.
  - $AB \subseteq A \cap B$.
- If A and B are ideals of a commutative ring R with unity and $A + B = R$, then $A \cap B = AB$.

  Proof: $a + b = 1,\ a_1 = b_1 = a_1a + a_1b = ab_1 + a_1b \in AB \Rightarrow A \cap B \subseteq AB$.

Theorem 14.1 Ideal Test

> A nonempty subset A of a ring R is an ideal of R if
>
> 1. $\forall a, b \in A,\ a - b \in A$.
> 2. $\forall a \in A, r \in R,\ ar, ra \in A$.

- Let a be an element of a commutative ring R, then the set $\langle a\rangle = \{ra \mid r \in R\}$ is an ideal of R called the **principal ideal** generated by a.
  - All polynomials with constant term 0, $A = \langle x\rangle$, is the subring of $\mathbb{R}[x]$.
  - If a is an idempotent, then a is the identity in the ideal $\langle a\rangle$.
  - If a, b belong to an integral domain, then $\langle a\rangle = \langle b\rangle$ if and only if $a = bu$ where u is a unit.
  - The characteristic of $\langle a\rangle$ is the additive order of a.
- Let $a_1, a_2, \cdots, a_n$ be elements of a commutatvive ring R, then $I = \langle a_1, a_2, \cdots, a_n\rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ is called the ideal generated by $a_1, a_2, \cdots, a_n$.
  - All polynomials with even constant terms, $I = \langle x, 2\rangle$, is the subring of $\mathbb{Z}[x]$.
- Let R be the ring of all real-valued functions of a real variable. The subset S of all differentiable functions is a subring of R but not an ideal of R.

14.2 Factor Rings

Theorem 14.2 Existence of Factor Rings

> Let R be a ring and let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

- R/I is a commutative ring with unity if and only if $rs - sr \in I$ for all r and s in R.
- R/I is a commutative ring with unity if R is commutative.

e.g.

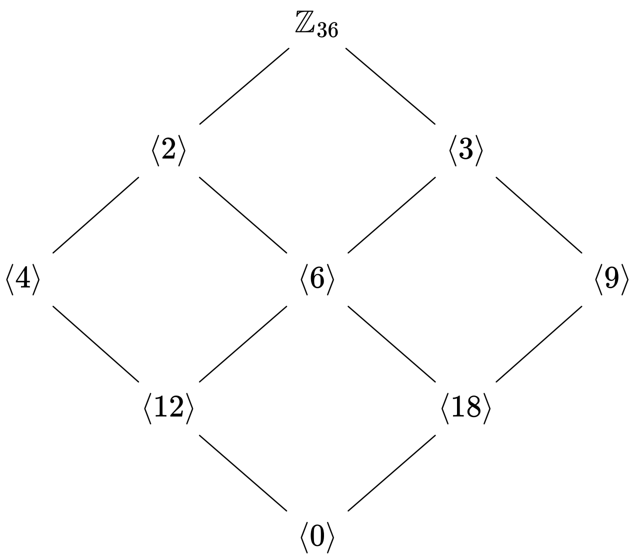
- $R = \mathbb{Z}_3[x]/\left\langle x^2 + 1\right\rangle$ is a cyclic group as well as a field of order 9.
- $R = \mathbb{Z}_5[x]/\left\langle x^2 + 1\right\rangle$ is not a field. $|R| = 25,\ |x + 1| = 4,\ (x + 2)(x + 3) = 0$.
- $|\mathbb{Z}[i]/\langle a + bi\rangle| = (a^2 + b^2)b$.

14.3 Prime Ideals and Maximal Ideals

Definition Prime Ideal, Maximal Ideal

> A **prime ideal** A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.
>
> A **maximal ideal** of a commutative ring R is a proper ideal A of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

- $n\mathbb{Z}$ is prime if and only if n is prime. ($\{0\}$ is also a prime ideal of $\mathbb{Z}$)
- $\langle s \rangle$ is a maximal ideal in $\mathbb{Z}_{st}$ if and only if s is prime.
- $\langle n \rangle$ is a maximal ideal in $\mathbb{Z}$ if and only if n is prime.
- The lattice of ideals of $\mathbb{Z}_{36}$ shows that both $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.



- From above we see that the intersection of prime ideals need not be a prime ideal.
- The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$. To prove this, assume A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2 + 1 \rangle$ and prove that $A = \mathbb{R}[x]$.
- The ideal $\langle x^2 + 1 \rangle$ is not prime in $\mathbb{Z}_2[x]$, since it contains $(x+1)^2 = x^2 + 1$ but not $x + 1$.
- If R is a finite commutative ring with unity, then every prime ideal of R is maximal.

Theorem 14.3 R/A Is an Integral Domain If and Only If A is Prime

> Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Proof $(a + A)(b + A) = ab + A = A \quad \Leftrightarrow \quad a + A = A \text{ or } b + A = A.$

Theorem 14.4 R/A is a Field If and Only If A Is Maximal

> Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only A is maximal.

- Maximal ideals are prime. ⭐
- From Examples to Theorem 14.2, we know that $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{Z}_3[x]$ but not prime in $\mathbb{Z}_5[x]$.
- The ideal $\langle x \rangle$ in $\mathbb{Z}[x]$ is prime but not maximal.
- $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field.

14.4 Exercises

1. $\langle 2\rangle$ is a maximal ideal of $\mathbb{Z}$ but $\langle 2\rangle[x]$ is not a maximal ideal of $\mathbb{Z}[x]$. $\langle 2, x\rangle$ is maximal.
2. In a commutative ring, the set of zero-divisors is an ideal.
3. Every nontrivial prime ideal of a finite commutative ring with unity is a maximal ideal. ⭐

   Proof: If P is prime in R, then R/P is a finite integral domain. Since a finite integral domain is a field, P is also maximal.
4. Every nontrivial prime ideal in a PID is a maximal ideal. ⭐
5. Every factor ring of a PID is a PID. ⭐

   Hint: Every factor ring of R/I has the form A/I, where A is a subring of R.
6. Let A be a subset of a commutative ring R, then
   1. The **annihilator** $\operatorname{Ann} A = \{r \in R \mid ra = 0 \text{ for all } a \text{ in } A\}$ is an ideal.
   2. The **nil radical** of A: $N(A) = \{r \in R \mid r^n \in A, n \in \mathbb{N}^+\}$ is an ideal.
   3. The nil radical of R: $N(\langle 0\rangle)$ is an ideal.
   4. $R/N(\langle 0\rangle)$ has no nonzero nilpotent elements.
   5. $N(N(A)) = N(A)$.

Confusion: 27

14.5 Bibliography of Richard Dedekind

14.6 Bibliography of Emmy Noether

15 Ring Homomorphisms

15.1 Definition and Examples

Definition Ring Homomorphism and Isomorphism

> A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,
>
> $$\phi(a+b) = \phi(a) + \phi(b)$$
> $$\phi(ab) = \phi(a)\phi(b).$$
>
> A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

- The natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$: $\phi : k \mapsto k \mod n$.
- To determine homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$, let $\phi(1) = a$ and notice that $a \cdot a = \phi(1 \cdot 1) = a$.
- Let R be a commutative ring of characteristic 2. Then the mapping $a \to a^2$ is a ring homomorphism from R to R.
- **Theorem of Gersonides**: The only case of positive integers when $2^m = 3^n + 1$ is for $(m, n) = (3, 2)$.

  In fact, it's the only solution in the natural numbers of $x^m - y^n = 1$ where $m, n, x, y > 1$.

15.2 Properties of Ring Homomorphisms

Theorem 15.1 Properties of Ring homomorphisms

> Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.
>
> 1. $\forall r \in R, n \in \mathbb{N}^+$, $\phi(nr) = n\phi(r)$, $\phi(r^n) = \phi(r)^n$.
> 2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.
> 3. If A is an ideal and ϕ is onto, then $\phi(A)$ is an ideal.
> 4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.
> 5. If R is commutative, then $\phi(R)$ is commutative.
> 6. If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S and units in R map to units in S.
> 7. ϕ is an isomorphism if and only if ϕ is onto and $\operatorname{Ker}\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.
> 8. If ϕ is an isomorphism from R to S, then ϕ^{-1} is an isomorphism from S onto R.

- The pullback of an ideal is an ideal, the converse is not true.
- Suppose that R and S are commutative rings with unities. Let ϕ be a ring homomorphism from R onto S and let B be an ideal of S.
  - If B is prime in S, then $\phi^{-1}(B)$ is prime in R.
  - If B is maximal in S, then $\phi^{-1}(B)$ is maximal in R.
- The homomorphic image of a principal ideal ring is a principal ideal ring.

Theorem 15.2 Kernels are Ideals

> Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\operatorname{Ker}\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.3 First Isomorphism Theorem for Rings

> Let ϕ be a ring homomorphism from R to S. Then the mapping $\psi : R/\operatorname{Ker}\phi \to \phi(R),\ r + \operatorname{Ker}\phi \mapsto \phi(r)$ is an isomorphism. In symbols, $R/\operatorname{Ker}\phi \approx \phi(R)$.

Proof Fundamental Theorem of Ring Homorphism

$$\begin{aligned}
\psi((x+\operatorname{Ker}\phi)+(y+\operatorname{Ker}\phi)) &= \psi(x+y+\operatorname{Ker}\phi) \\
&= \phi(x+y) = \phi(x)+\phi(y) \\
&= \psi(x+\operatorname{Ker}\phi)+\psi(y+\operatorname{Ker}\phi) \\
\psi((x+\operatorname{Ker}\phi)(y+\operatorname{Ker}\phi)) &= \psi(xy+\operatorname{Ker}\phi) \\
&= \phi(xy) = \phi(x)\phi(y) \\
&= \psi(x+\operatorname{Ker}\phi)\psi(y+\operatorname{Ker}\phi)
\end{aligned}$$

Corollary 1 Second Isomorphism Theorem for Rings

> If A is a subring of R and B is an ideal of R, then $A/(A\cap B) \approx AB/B$.

Proof Let $\phi : A \to AB/B,\ a \mapsto aB$, then $\operatorname{Ker}\phi = A \cap B$.

Corollary 2 Third Isomorphism Theorem for Rings

> If A and B are ideals of R and $B \subseteq A$, then $(S/B)/(A/B) \approx S/A$.

Proof Let $\phi : S/B \to S/A,\ sB \mapsto sA$, then $\operatorname{Ker}\phi = A/B$.

Theorem 15.4 Ideals are Kernels

> Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the **natural mapping** $\phi : R \to R/A,\ r \mapsto r + A$.

- $\mathbb{Z}[x]/\langle x\rangle \approx \mathbb{Z}$, and because $\mathbb{Z}$ is an integral domain but not a field, the ideal $\langle x\rangle$ is prime but nor maximal in $\mathbb{Z}[x]$.

Theorem 15.5 Homomorphism from $\mathbb{Z}$ to a Ring with Unity

> Let R be a ring with unity 1. The mapping $\phi:\mathbb{Z}\to R,\ n\mapsto n\cdot 1$ is a ring homomorphism.

Corollary 1 A Ring with Unity Contains $\mathbb{Z}_n$ or $\mathbb{Z}$

> If R is a ring with unity and the characteristic of R is $n>0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 2 $\mathbb{Z}_m$ Is a Homomorphic Image of $\mathbb{Z}$

> For any positive integer m, the mapping of $\phi:\mathbb{Z}\to\mathbb{Z}_m,\ x\mapsto x \mod m$ is a ring homomorphism.

Corollary 3 A Field Conatins $\mathbb{Z}_p$ or $\mathbb{Q}$

> If $\mathbb{F}$ is a field of characteristic p, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a subfield isomorphic to $\mathbb{Q}$.

Since the intersection of all subfields of a field is itself a subfield, and every field has a smallest subfield, which is called the **prime subfield** of the field. The prime subfield is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Q}$.

15.3 The Field of Quotients

Theorem 15.6 Field of Quotients

> Let $\mathbb{D}$ be an integral domain. Then there exists a field $\mathbb{F}$ (called the **field of quotients** of $\mathbb{D}$) that contains a subring isomorphic to $\mathbb{D}$.

Proof Let $S=\{(a,b)\mid a,b\in\mathbb{D}, b\neq 0\}$, we define an equivalence relation on S by $(a,b)\equiv(c,d)$ if $ad=bc$, denote the equivalence class that contains (x,y) by x/y, and define addition and multiplication on $\mathbb{F}$ by

$$a/b+c/d=(ad+bc)/(bd) \text{ and } a/b\cdot c/d=(ac)/(bd).$$

Then the mapping $\phi:\mathbb{D}\to\mathbb{F},\ x\mapsto x/1$ is a ring isomorphism. □

- When $\mathbb{F}$ is a field , the field of quotients of $\mathbb{F}[x]$ is traditionally denoted by $\mathbb{F}(x)$.
- Let p be a prime, then $\mathbb{Z}_p(x)=\{f(x)/g(x)\mid f(x),g(x)\in\mathbb{Z}_p[x], g(x)\neq 0\}$ is an infinite field of characteristic p.
- The field of quotients of a field $\mathbb{F}$ is ring-isomorphic to $\mathbb{F}$.
- The field of quotients of an integral domain $\mathbb{D}$ is the smallest field containing $\mathbb{D}$.

15.4 Exercises

1. Examples
    1. Let $S=\left\{\begin{bmatrix} a & b\\ bd & a\end{bmatrix}\,\middle|\, a,b\in\mathbb{R}\right\}$, $d\in\mathbb{Z}$, then $\phi:\mathbb{Z}[\sqrt{d}]\to S,\ a+b\sqrt{d}\mapsto\begin{bmatrix} a & b\\ bd & a\end{bmatrix}$ is a ring isomorphism.
    2. $\phi:\mathbb{Z}_m\to\mathbb{Z}_n,\ x\mapsto x \mod n$ is a ring homomorphism if and only if $n\mid m$.
    3. $\phi:\mathbb{Z}_{mn}\to\mathbb{Z}_p\oplus\mathbb{Z}_n,\ x\mapsto(x \mod m,\ x \mod n)$ where $\gcd(m,n)=1$.

4. $\phi: \mathbb{Z}_m \to \mathbb{Z}_n,\ x \mapsto ax$ where $n \mid m$ and a is an idempotent of $\mathbb{Z}_n$.
5. $\phi: \mathbb{Z}[\mathrm{i}]/\langle a+b\mathrm{i}\rangle \to \mathbb{Z}[\mathrm{i}]/\langle a-b\mathrm{i}\rangle,\ z+\langle a+b\mathrm{i}\rangle \mapsto z+\langle a-b\mathrm{i}\rangle$ where a and b are nonzero real numbers.
6. Let $R=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a,b \in \mathbb{Z}\right\}$, then
   $\phi: R \to \mathbb{Z},\ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mapsto a-b$ is a ring homomorphism.

2. Both $\phi: \mathbb{Z}\oplus\mathbb{Z} \to \mathbb{Z},\ (a,b) \mapsto a$ and $\psi: \mathbb{Z}_6 \to \mathbb{Z}_6,\ x \mapsto 3x$ take a zero-divisor to the unity.
3. If $\phi: R \to S$ is onto and $\operatorname{char} R \neq 0$, then $\operatorname{char} S \mid \operatorname{char} R$.
4. Let R be a commutative ring of prime characteristic p, then the **Frobenius map** $x \mapsto x^p$ is a ring homomorphism from R to R. If R is a field, then the mapping is an isomorphism.

16 Polynomial Rings

16.1 Notation and Terminology

Definition Ring of Polynomials over R

> Let R be a commutative ring. The set of formal symbols
>
> $$R[x]=\left\{a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \mid a_i \in R, n \in \mathbb{N}\right\},$$
>
> is called the ring of polynomials over R in the **indeterminate** x. Two elements $a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ and $b_m x^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$ of $R[x]$ are considered equal if and only if $a_i=b_i$ for all nonnegative integers i. (Define $a_i=0$ when $i>n$ and $b_m=0$ when $i>m$.)

Definition Addition and Multiplication in $R[x]$

- For $f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\ a_n \neq 0$, the **degree** is n, denoted by $\deg f(x)$, and the **leading coefficient** is a_n. If a_n is the unity, then $f(x)$ is a **monic** polynomial.
- In an integral domain, $\deg(f(x)g(x))=\deg(f(x))+\deg(g(x))$, but it is possible that $\deg(f(x)g(x))<\deg(f(x))+\deg(g(x))$.

Theorem 16.1 $\mathbb{D}$ an Integral Domain Implies $\mathbb{D}[x]$ an Integral Domain

> If $\mathbb{D}$ is an integral domain, then $\mathbb{D}[x]$ is an integral domain.

- Since $\mathbb{D}[x]$ is a ring, we only need to prove that $\mathbb{D}[x]$ is commutative with a unity and has no zero-divisors.

16.2 The Division Algorithm and Consequences

Theorem 16.2 Division Algorithm for $F[x]$

> Let F be a field and let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x)=g(x)q(x)+r(x)$ where either $r(x)=0$ or $\deg r(x)<\deg g(x)$.

- Long division process, which is also true for integral domains.

- If $f(x) = g(x)h(x)$, we write $g(x) \mid f(x)$ and call $g(x)$ a **factor** of $f(x)$.
- An element a is a **zero** (or a **root**) of $f(x)$ if $f(a) = 0$, and we say that a is a **zero of multiplicity** k if $(x-a)^k \mid f(x)$ but $(x-a)^{k+1} \nmid f(x)$.

Corollary 1 Remainder Theorem

> Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 2 Factor Theorem

> Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

- It's also true over any commutative ring with unity.

Theorem 16.3 Polynomials of Degree n Have at Most n Zeros

> A polynomial of degree n over a field has at most n zeros, counting multiplicity.

- It's also true over integral domains.
- In the ring $\mathbb{Z}_8[x]$, $x^2 + 7$ has $1, 3, 5, 7$ as zeros. ($\mathbb{Z}_p[x]$ is a field.)
- A **primitive n^{th} root of unity**: $\omega = \mathrm{e}^{\mathrm{i}\pi/n}$.

Definition Principal Ideal Domain (PID)

> A **principal ideal domain** is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some a in R.

Theorem 16.4 $F[x]$ Is a PID

> Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a principal ideal domain.

- If a field $\mathbb{F}$ has an ideal I, then $I = \{0\}$ or $\mathbb{F}$.

  Proof If $\exists a \in I, a \neq 0$, then $a \cdot a^{-1} = 1 \in I$, so $\forall x \in \mathbb{F},\ x = x \cdot 1 \in I$.
- $\mathbb{Z}[x]$ is an iconic integral domain of polynomials, but it's not PID, because the ideal of all elements in $\mathbb{Z}[x]$ with even constant term is not generated by a single element.

Theorem 16.5 Criterion for $I = \langle g(x) \rangle$

> Let $\mathbb{F}$ be a field, I a nonzero ideal in $\mathbb{F}[x]$, and $g(x)$ an element of $\mathbb{F}[x]$. Then $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

- $\phi : \mathbb{R}[x] \to \mathbb{C},\ f(x) \mapsto f(\mathrm{i})$, then $x^2 + 1 \in \operatorname{Ker} \phi$ and is of minimum degree. Thus, $\operatorname{Ker} \phi = \langle x^2 + 1 \rangle$ and $\mathbb{R}[x] / \langle x^2 + 1 \rangle \approx \mathbb{C}$.

16.3 Exercises

Wilson's Theorem

> For every integer $n > 1$, $(n-1)! \mod n = -1$ if and only if n is prime.

- $(p-2)! \mod p = 1$.

---

1. Every element in the ring of polynomial functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ can be written in the form $a_{p-1}x^{p-1} + \cdots + a_0$.
2. $R \approx S \Leftrightarrow R[x] \approx S[x]$. ⭐

1. If $\phi : R \to S$ is a ring homomorphism, then $\bar{\phi} : R[x] \to S[x],\ (a_n x^n + \cdots + a_0) \to \phi(a_n)x^n + \cdots + \phi(a_0)$ is also a ring homomorphism.
2. $\phi : R[x] \to R,\ f(x) \mapsto f(r)$ is called the **evaluation homomorphism**.

3. $U(p)$ is cyclic.

   Proof: For $p > 3$, otherwise $U(p)$ has a subgroup isomorphic to $\mathbb{Z}_q \oplus \mathbb{Z}_q$ where q is a prime. But then $x^q - 1$ in $\mathbb{Z}_q[x]$ has $q^2 - 1$ zeros.

4. In $\mathbb{Z}_p[x]$, $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$.

5. Relation between a ring and a polynomial ring ⭐

   1. I is an ideal of a ring $R \quad \Leftrightarrow \quad I[x]$ is an ideal of $R[x]$.
   2. I is a maximal ideal of a ring $R \quad \not\Rightarrow \quad I[x]$ is a maximal ideal of $R[x]$.
   3. I is a prime ideal of a ring $R \quad \Rightarrow \quad I[x]$ is a prime ideal of $R[x]$.

6. If there is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{F}$, then $\mathbb{F} \approx \mathbb{Z}_p$.

7. Suppose $f(x)$ is a polynomial with odd coefficients and even degree, then $f(x)$ has no rational zeros. 🌙

   Hint: Analog of the proof that $\sqrt{2}$ is irrational.

Confusion: 8

17 Factorization of Polynomials

17.1 Reducibility Tests

Definition Irreducible Polynomial

> Let $\mathbb{D}$ be an integral domain. A polynomial $f(x)$ from $\mathbb{D}[x]$ that is neither the zero polynomial nor a unit in $\mathbb{D}[x]$is said to be **irreducible** over $\mathbb{D}$ if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ from $\mathbb{D}[x]$, then $g(x)$ or $h(x)$ is a unit in $\mathbb{D}[x]$. A nonzero, nonunit element of $\mathbb{D}[x]$ that is not irreducible over D is called reducible over D.

Theorem 17.1 Reducibility Test for Degrees 2 and 3

> Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and $\deg f(x) = 2$ or 3, then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in $\mathbb{F}$.

- In $\mathbb{Q}[x]$, $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$, $x^4 + 2x^2 + 1 = (x^2+1)^2$, and in $\mathbb{R}[x]$, $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

Definition Content of a Polynomial, Primitive Polynomial

> The **content** of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where the a's are integers, is the greatest common divisor of $a_n, a_{n-1}, \cdots, a_0$. A **primitive polynomial** is an element of $\mathbb{Z}[x]$ with content 1.

Gauss's Lemma

> The product of two primitive polynomials is primitive.

Theorem 17.2 Reducibility over $\mathbb{Q}$ Implies Reducibility over $\mathbb{Z}$

Let $f(x) \in \mathbb{Z}[x]$, if $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

- If $f(x)$ is irreducible over $\mathbb{Z}$, then it's irreducible over $\mathbb{Q}$.
- $f(x) = 2(x^2+1)$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$ since 2 is not a unit of $\mathbb{Z}$.

17.2 Irreducibility Tests

Theorem 17.3 Mod p Irreducibility Test

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

- To prove it: if $f(x)$ is reducible over $\mathbb{Q}$, then it's reducible over $\mathbb{Z}_p$.

Theorem 17.4 Eisenstein's Criterion

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n, p \mid a_{n-1}, \cdots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary Irreducibility of p^{th} Cyclotomic Polynomial

For any prime p, the p^{th} **cyclotomic polynomial**

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Proof $\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}$ is irreducible over $\mathbb{Q}$.

Theorem 17.5 $\langle p(x) \rangle$ Is Maximal If and Only If $p(x)$ Is Irreducible

Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over $\mathbb{F}$.

Corollary 1 $\mathbb{F}[x]/\langle p(x) \rangle$ Is a Field

Let $\mathbb{F}$ be a field and $p(x)$ be an irrducible polynomial over $\mathbb{F}$, then $\mathbb{F}[x]/\langle p(x) \rangle$ is a field.

- This follows directly from Theorem 14.4 and 17.5.

Corollary 2 $p(x) \mid a(x)b(x)$ Implies $p(x) \mid a(x)$ or $p(x) \mid b(x)$

Let $\mathbb{F}$ be a field and let $p(x), a(x), b(x) \in \mathbb{F}[x]$. If $p(x)$ is irreducible over $\mathbb{F}$ and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

- To construct a field with p^n elements, find a polynomial of degree n with no zero in $\mathbb{Z}_p$, say $P_n(x)$, then $\mathbb{Z}_p[x]/P_n(x)$ satisfies.

17.3 Unique Factorization in $\mathbb{Z}[x]$

- The only units in $\mathbb{Z}[x]$ are ± 1.
- The irreducible polynomials of degree 0 over $\mathbb{Z}$ are $f(x) = \pm p$ where p is a prime.
- Every nonconstant irreducible polynomial from $\mathbb{Z}[x]$ is primitive.

Theorem 17.6 Unique Factorization in $\mathbb{Z}[x]$

> Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form
>
> $$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x),$$
>
> *uniquely* where the b_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s are irreducible polynomials of positive degree.

17.4 Weird Dice: An Application of Unique Factorization

1, 2, 2, 3, 3, 4

1, 3, 4, 5, 6, 8

17.5 Exercises

Rational Root Theorem

> Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ $(a_n \neq 0)$, if $f(r/s) = 0$ where r and s are relatively prime integers, then $r \mid a_0,\ s \mid a_n$.

Proof i.e. $a_n r^m + a_{n-1} s r^{n-1} + \cdots + a_0 s^n = 0$. This shows that $s \mid a_n r^n$ and $r \mid s^n a_0$. ☐

---

1. In $\mathbb{Z}_p[x]$, $ax^2 + bx + c = 0 \Leftrightarrow (2ax + b)^2 = b^2 - 4ac$, if $\sqrt{b^2 - 4ac}$ has at least one solution, then the quadratic formula $x = (-b \pm \sqrt{b^2 - 4ac}) \cdot (2a)^{-1}$ holds.
2. The number of reducible polynomials of degree n over $\mathbb{Z}_p$ is $p\left(\mathrm{C}_p^n + p\right)$.

Better Solution: 8, 14.e,

17.6 Bibliography of Serge Lang

18 Divisibility in Integral Domains

18.1 Irreducibles, Primes

Definition Associates, Irreducibles, Primes

> Elements a and b of an integral domain D are called **associates** if $a = ub$, where u is a unit of D.
>
> A nonzero element a of an integral domain D is called an **irreducible** if a is not a unit and whenever $a = bc,\ b, c \in D$, then b or c is a unit.
>
> A nonzero element a of an integral domain D is called a **prime** if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

- **associates**
  - equivalence relation: $a \sim b$ if $a = ub$.
  - $a = ub \quad \Leftrightarrow \quad \langle a \rangle = \langle b \rangle$.
- **irreducible**

- The product of an irreducible and a unit is an irreducible.

- **prime**
  - a if a prime if and only if $\langle a \rangle$ is a prime ideal.
- **norm**

  $\mathbb{Z}[\sqrt{d} >] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$, where $d \neq 1$ and not divisible by the square of a prime. Define a function called the **norm**: $N : \mathbb{Z}[\sqrt{d} >] \to \mathbb{N},\ a + b\sqrt{d} \mapsto |a^2 - db^2|$, then

  1. $N(x) = 0$ if and only if $x = 0$.
  2. $N(xy) = N(x)N(y)$.
  3. x is a unit if and only if $N(x) = 1$.
  4. If $N(x)$ is prime, then x is irreducible.

     The converse is not true.

  - If $d < -1$, then the only units of $\mathbb{Z}[\sqrt{d} >]$ is ± 1.

e.g.

- In $\mathbb{Z}[\sqrt{-3} >]$, $1 + \sqrt{-3}$ is an irreducible, but not a prime. (Consider $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4$, but $1 + \sqrt{-3} \nmid 2$.)
- To show that $a_0 + b_0\sqrt{d}$ is irreducible, notice that every solution of $a^2 - db^2 = c$ would also hold in $\mathbb{Z}_n$, just try to find a counter-example.

Theorem 18.1 Prime Implies Irreducible

> In an integral domain, every prime is an irreducible.

Proof If $a = bc$, then $a \mid b$ or $a \mid c$. Let $b = at = bct$, then $1 = ct$, thus c is a unit. ☐

Theorem 18.2 PID Implies Irreducible Equals Prime

> In a principal ideal domain, en element is an irreducible if and only if it is prime.

Proof Suppose $a \mid bc$, consider the ideal $I = \{ax + by \mid x, y \in D\} = \langle d \rangle$. Let $a = dr$, then d is a unit or r is a unit.

1. If d is a unit, then $I = D$ and $1 = ax + by \Rightarrow c = acx + bcy$, and since $a \mid bc$, we have $a \mid c$.
2. If r is a unit, then $I = \langle d \rangle = \langle a \rangle$, and we have $at = b$, thus $a \mid b$. ☐

- This theorem holds in a UFD.
- $\mathbb{Z}[x]$ is not a principal ideal domain since we have the ideal $I = \langle 2, x \rangle$.

18.2 Historical Discussion of Fermat's Last Theorem

18.3 Unique Factorization Domains

Definition Unique Factorization Domain (UFD)

> An integral domain D is a **unique factorization domain** if
>
> 1. every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and

2. the factorization into irreducibles is unique up to *associates* and the order in which the factors appear.

- $\mathbb{C}$ is not a UFD since $5 = (2+\mathrm{i})(2-\mathrm{i}) = (1+2\mathrm{i})(1-2\mathrm{i})$.

Lemma *Ascending Chain Condition* for a PID

> In a principal ideal domain, any strictly increasing chian of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length.

Proof Let $I = I_1 \cup I_2 \cup \cdots = \langle a \rangle$, say $a \in I_n$, then $I_i \subseteq I = \langle a \rangle \subseteq I_n$, so that I_n is the last member of the chain. $\square$

Theorem 18.3 PID Implies UFD

> Every principal ideal domain is a unique factorization domain.

- An integral domain with the property that there is no infinite, strictly increasing chain of ideals in D, is called a **Noetherian domain**.
- $\mathbb{Z}[x]$ is a Noetherian domain and also a UFD, but not a PID.

Corollary $\mathbb{F}[x]$ Is a UFD

> Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a unique factorization domain.

We can prove the Eisentein's Criterion by this corollary elegantly.

18.4 Euclidean Domains

Definition Euclidean Domain (ED)

> An integral domain D is called a **Euclidean domain** if there is a function d (called the **measure**) from the nonzero elements of D to the nonnegative integers such that
>
> 1. $d(a) \leq d(ab)$ for all nonzero a, b in D; and
> 2. if $a, b \in D,\ b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

- u is a unit $\quad\Leftrightarrow\quad d(u) = d(1)$.
- $a = ub \quad\Rightarrow\quad d(a) = d(b)$.
- The subdomain of an ED may not be an ED.
- Similarities Between $\mathbb{Z}$ and $\mathbb{F}[x]$.

Properties	$\mathbb{Z}$	$\mathbb{F}[x]$
Euclidean Domain	$d(a) = \|a\|$.	$d(f(x)) = \deg f(x)$.
Units	If and ony if $\|a\| = 1$.	If and only if $\deg f(x) = 0$.
Division Algorithm	$a = bq + r$.	$f(x) = g(x)q(x) + r(x)$.
Principal Ideal Domain	$I = \langle a \rangle$ where $\langle a \rangle$ is minimum.	$I = \langle f(x) \rangle$ where $\deg f(x)$ is minimum.
Prime	No nontrivial factors.	No nontrivial factors.

Properties	$\mathbb{Z}$	$\mathbb{F}[x]$
Unique Factorization Domain	Every element is a unique product of primes.	Every element is a unique product of irreducibles.

- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain with $d(a + bi) = a^2 + b^2$.
  1. $d(x) \leq d(xy)$ follows directly from $d(xy) = d(x)d(y)$.
  2. Say $xy^{-1} = s + t\mathrm{i},\ s, t \in \mathbb{Q}$, let m be the integer nearest s, and n be the integer nearest t, then

     $xy^{-1} = (m + n\mathrm{i}) + [(s - m) + (t - n)\mathrm{i}]$,

     $x = (m + n\mathrm{i})y + r,\ r = [(s - m) + (t - n)\mathrm{i}]y$,

     $d(r) \leq (\frac{1}{4} + \frac{1}{4})d(y) < d(y)$.
  - $\mathbb{Z}[\mathrm{i}]/I$ is finite.
- $\mathbb{Z}[\sqrt{d}]$ is Euclidean domain when $d = \pm 2, \pm 1$, and there are no other negative values that satisfy.

Theorem 18.4 ED Implies PID

> Every Euclidean domain is a principal ideal domain.

Proof The zero ideal is $\langle a \rangle$. For a nonzero ideal I, let $a \in I$ be such that $d(a)$ is a minimum, then $I = \langle a \rangle$. For, $\forall b \in I,\ b = aq + r$, but $r = b - aq \in I$, so $d(r) \geq d(a)$, thus $r = 0$ and $b \in \langle a \rangle$.
☐

- There are PID that are not ED.

Corollary ED Implies UFD

> Every Euclidean domain is a unique factorization domain.

$$ED \Rightarrow PID \Rightarrow UFD,$$
$$UFD \nRightarrow PID \nRightarrow ED.$$

Theorem 18.5 D a UFD Implies $D[x]$ a UFD

> If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

- $\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not a PID.
- $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD,

  since $46 = 2 \cdot 23 = (1 + 3\sqrt{-5})(1 - 3\sqrt{-5})$.

18.5 Exercises

1. Suppose a and b belong to an integral domain and $b \neq 0$, then

   $\langle ab \rangle$ is a proper subset of $\langle b \rangle \quad \Leftrightarrow \quad a$ is not a unit.
2. Every proper ideal of a PID is contained in its maximal ideal.
3. In $\mathbb{Z}_n$ where n need not to be a prime,
   1. $p \mid n \quad \Leftrightarrow \quad p$ is prime in $\mathbb{Z}_n$.
   2. $p^2 \mid n \quad \Leftrightarrow \quad p$ is irreducible in $\mathbb{Z}_n$ and $p \mid n$.

4. *Descentding chain condition*

   An integral domain with the property that every strictly decreasing chain of ideals $I_1 \supset I_2 \supset \cdots$ must be finite in length is a field.

5. An ideal A of a commutative ring R with unity is said to be **finitely generated** if there exist elemts $a_1, a_2, \cdots, a_n$ of A such that $A = \langle a_1, a_2, \cdots, a_n \rangle$.

   An integral domain R satisfies the ascending chain condition. $\Leftrightarrow$ Every ideal of R is finitely generated.

6. For every field $\mathbb{F}$, there are infinitely many irreducibles in $\mathbb{F}[x]$.

7. Let I be a non-zero ideal in a PID R, then R/I has a fiinte number of ideals.

Question:

- 30, $\Rightarrow$.

18.6 Bibliography of Sophie Germain

18.7 Bibliography of Andrew Wiles

18.8 Bibliography of Pierre de Fermat