Chapter - 3 : Ring Theory

Definition .41 *A ring is an ordered pair $(R,+,*)$ where R is a non-empty set, and $+$ and $*$ are two binary operations on R satisfying the following axioms:*

A1 $a+b \in R$ *for all* $a,b \in R$ *(closure).*

A2 $(a+b)+c = a+(b+c)$ *for all* $a,b,c \in R$ *(associativity).*

A3 *There exists* $0 \in R$ *such that* $a+0 = a = 0+a$ *for all* $a \in R$ *(identity).*

A4 *For every* $a \in R$*, there exists* $b \in R$ *such that* $a+b = 0 = b+a$ *(additive inverse).*

A5 $a+b = b+a$ *for all* $a,b \in R$ *(commutativity).*

M1 $ab \in R$ *for all* $a,b \in R$ *(closure).*

M2 $(ab)c = a(bc)$ *for all* $a,b,c \in R$ *(associativity).*

M3 1. $a\cdot(b+c) = a\cdot b + a\cdot c$ *(left distributive law).*

2. $(a+b)\cdot c = a\cdot c + b\cdot c$ *(right distributive law).*

$(R,+,*)$ *is called a commutative ring if for all* $a,b \in R$*,* $ab = ba$*; otherwise, it is non-commutative.* R *is called a ring with unity if there exists* $1 \in R$ *such that* $1\cdot a = a = a\cdot 1$ *for all* $a \in R$*, where* 1 *is referred to as the unity of* R*; otherwise,* R *is a ring without unity.*

Example 1.10.6 1. *The rings* $\mathbb{Z}$ *and* $\mathbb{Q}$ *have unity, but* $2\mathbb{Z}$ *does not.*

2. *Consider the set* M *of all matrices* $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *where* $a,b,c,d \in \mathbb{Z}$*. This set forms a ring under matrix addition and multiplication.* M *is a non-commutative ring with unity, where* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ *serves as the unity element.*

3. *The set* F *of all continuous functions* $f : \mathbb{R} \to \mathbb{R}$ *is an infinite ring with unity.*

4. *The set of integers modulo 6, denoted* $\mathbb{Z}_6$*, forms a ring under addition modulo 6 and multiplication modulo 6.*

5. *The set of integers modulo n, denoted* $\mathbb{Z}_n$*, is a ring.*

6. *For a non-empty set* X*, the set* $P(X)$ *of subsets of* X *is a ring under the following operations:*

   (a) $A+B = (A\setminus B)\cup(B\setminus A)$ *for all* $A,B \in P(X)$.

   (b) $AB = A\cap B$ *for all* $A,B \in P(X)$.

   $P(X)$ *is a commutative ring with unity, where the unity is the set* X *itself.*

7. *Given two rings* R_1 *and* R_2*, the set* $R_1\times R_2 = \{(a,b) \,:\, a\in R_1, b\in R_2\}$*, with operations defined as follows:*

   (a) $(a+b)+(c+d) = (a+c, b+d)$

   (b) $(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$

   This is called the direct product of R_1 *and* R_2*. The product* $R_1\times R_2$ *is commutative if and only if both* R_1 *and* R_2 *are commutative. Similarly,* $R_1\times R_2$ *has unity if and only if both* R_1 *and* R_2 *have unity.*

1.11. Integral Domain

Definition .42 *Let* $(R,+,*)$ *be a ring. An element* $a \in R$ *is called a left zero divisor if there exists* $b \neq 0 \in R$ *such that* $ab = 0$*.*

Similarly, we define a right zero divisor. If $ab = 0 = ba$*, then* a *is simply a zero divisor. If* a *is a zero divisor, then* b *is also. If* $a \neq 0$*, then it is a proper zero divisor.*

Proposition .20 *R has no zero divisors if and only if the left/right cancellation law holds.*

Hint(s): $ab = ac \Rightarrow a(b-c) = 0$. *If* $a \neq 0$ *and* $b - c \neq 0$, *no cancellation law is possible.*

Definition .43 *A commutative ring R is said to be an integral domain if it has no zero divisors.*

We include, in the definition of an integral domain, that R has unity (for convenience).

Example 1.11.1
1. $\mathbb{Z}$ *is an integral domain.*
2. $\mathbb{Z}_6$ *is not an integral domain since* 2 *is a zero divisor in* $\mathbb{Z}_6$.

Exercise 34 $\mathbb{Z}_n$ *is an integral domain if and only if n is prime.*

Hint(s): *Assume n is prime. Let* $[a]_n$ *and* $[b]_n$ *be nonzero residue classes in* $\mathbb{Z}_n$. *If* $[a]_n \cdot [b]_n = [0]_n$, *then* $ab \equiv 0 \pmod{n}$, *implying n divides ab. Since n is prime, this implies n divides a or n divides b, which contradicts their being nonzero residue classes. Hence,* $\mathbb{Z}_n$ *has no zero divisors, making it an integral domain.*

(If $\mathbb{Z}_n$ *is an integral domain, then n is prime):*

Assume $\mathbb{Z}_n$ *is an integral domain. Suppose n is composite, so* $n = ab$ *for* $1 < a, b < n$. *Then,* $[a]_n \cdot [b]_n = [ab]_n = [0]_n$, *showing that* $\mathbb{Z}_n$ *has zero divisors, which is a contradiction. Therefore,* $\mathbb{Z}_n$ *being an integral domain implies n is prime.*

Note 20 *Invertible elements of R are called units.*

Definition .44 (Skew Field or Division Ring) *A ring R is called a division ring if every non-zero element of R has an inverse (i.e., is a unit).*

Proposition .21 *If R is a division ring, then all non-zero elements of R form a group under multiplication.*

Proof:

Theorem .29 *If R is a ring with 1, then all units of R form a group (under multiplication).*

Proof: *Define* $U = \{a \in R \mid \exists\ x \text{ such that } ax = 1 = xa\}$. *Let* $a, b \in U$, *i.e.,* $\exists\ x, y \in U$ *such that* $ax = 1 = xa$, *and* $by = 1 = yb$. *Consider*

$$(ab)(yx) = a(by)x = a(1)x = ax = 1$$
$$(yx)(ab) = y(xa)b = y(1)b = yb = 1$$

Thus, ab is a unit. Also, for all $a \in U$, *there exists* $x \in R$ *such that* $ax = 1 = xa$. *Now,* $a^{-1}x^{-1} = (xa)^{-1} = 1^{-1} = 1$ *since* $x^{-1}a^{-1} = 1$.

Note 21 *A commutative division ring is a field.*

Example 1.11.2 $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ *are fields.*

Proposition .22 *Every field is an integral domain.*

Proof: *Let F be a field, i.e., for every* $x \neq 0$ *in F, there exists* $y = x^{-1}$ *such that* $xy = 1 = yx$. *Suppose, for contradiction, that there exists* $a \in F$ *such that* $b \neq 0$ *and* $ab = 0$, *but also* a^{-1} *exists in F. Multiplying both sides by* a^{-1}, *we get* $a^{-1}(ab) = a^{-1}(0) \Rightarrow b = 0$, *leading to a contradiction. Thus, F has no zero divisors and is an integral domain.*

Remark 3 *The converse of the above proposition is not true in general.* $\mathbb{Z}$ *is an integral domain but not a field.*

Theorem .30 *Every finite integral domain is a field.*

Proof: *Let R be a finite integral domain. Consider* $R = \{a_1, a_2, \ldots, a_n\}$ *for* $0 \neq a \in R$. *Define* $aR = \{aa_1, aa_2, \ldots, aa_n\}$. *Since* $1 \in R$, *there exists* $aa_i \in aR$ *such that* $1 = aa_i$ *for some i. This implies that every nonzero element in R has a multiplicative inverse. Therefore, all elements of R are units, making R a field.*

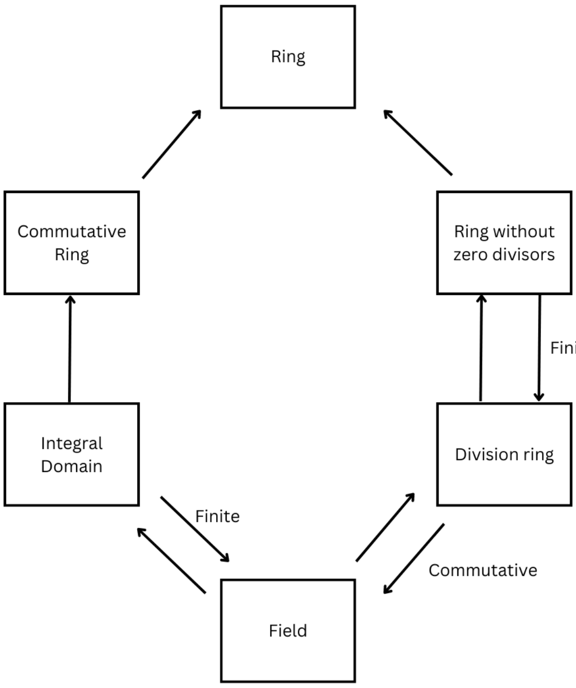
Exercise 35 *Prove that* $\mathbb{Z}_n$ *is a field if and only if n is prime.*

Definition .45 (Characteristic) *Let R be a ring. The smallest positive integer n such that* $na = 0$ *for all* $a \in R$ *is called the characteristic of R.*

If there is no nonzero n such that $na = 0$, then $Char(R) = 0$.

Theorem .31 *The characteristic of an integral domain is either prime or zero.*

Proof: *Let $Char(R) = n$ for an integral domain R. Suppose n is not prime, i.e., $n = ab$ where $1 < a, b < n$. Since $nx = 0$ for all $x \in R$, it implies $(ab)x = 0$ for all $x \in R$. But R being an integral domain contradicts this, as either $a \cdot 1 = 0$ or $b \cdot 1 = 0$, which cannot hold due to the minimality of n for which $nx = 0$. Thus, n must be prime. If $n = 0$, the result is trivially true.*



Definition .46 (Gaussian Integers Ring) *Let $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$. Then, $\mathbb{Z}[i]$ is called the ring of Gaussian integers.*

Proposition .23 *$\mathbb{Z}[i]$ is an integral domain under the operations:*

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$
$$(a+ib)\cdot(c+id) = (ac-bd)+i(ac+bd)$$

Proof: *Assume $xy = 0$ for all $0 \neq x, 0 \neq y \in \mathbb{Z}[i]$, where $x = a+ib$ and $y = c+id$. This implies $ac-bd = 0$ and $ad+bc = 0$, leading to $bd^2 + bc^2 = 0$. This implies $d^2 + c^2 = 0$ or $b = 0$. This means either $a = 0$ or $c = 0$, which is a contradiction. Hence, $\mathbb{Z}[i]$ has no zero divisors, and therefore, it is an integral domain.*

Exercise 36 *Prove that $\mathbb{Z}[i]$ is a ring with unity.*

Example 1.11.3 *Units of $\mathbb{Z}[i]$.*

Proof: *Let $a+ib$ and $c+id$ be arbitrary elements in $\mathbb{Z}[i]$. Consider the equation $(a+ib)(c+id) = 1$, which implies $(a-ib)(c-id) = 1$.*

Multiplying these expressions, we get $(a^2+b^2)(c^2+d^2) = 1$. This equation has only one possibility: $a^2+b^2 = d^2+c^2 = 1$.

In the first case, $a^2+b^2 = 1$ implies $a = \pm 1$ and $b = 0$, and similarly, $c^2+d^2 = 1$ implies $c = \pm 1$ and $d = 0$. In the second case, $b = \pm 1$ and $a = 0$ from $a^2+b^2 = 1$, and similarly, $d = \pm 1$ and $c = 0$ from $d^2+c^2 = 1$.

Therefore, the only units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Example 1.11.4 *Find the roots of x^2+3x-4 in $\mathbb{Z}_6$.*

Solution: *Since $(x-1)(x+4) = 0$ in $\mathbb{Z}_6$, the possibilities are:*

1. $x-1 \equiv 0 \Rightarrow x \equiv 1$ *(possible).*
2. $x-1 \equiv 2$ *and* $x+4 \equiv 3 \Rightarrow x \equiv 3$ *and* $x \equiv 5$ *(impossible).*
3. $x-1 \equiv 3$ *and* $x+4 \equiv 2 \Rightarrow x \equiv 4$ *and* $x \equiv 4$ *(possible).*
4. $x+4 \equiv 0 \Rightarrow x \equiv 2$ *(possible).*
5. $x-1 \equiv 1$ *and* $x+4 \equiv 6 \Rightarrow x \equiv 2$ *and* $x \equiv 2$ *(possible).*
6. $x-1 \equiv 6$ *and* $x+4 \equiv 2 \Rightarrow x \equiv 1$ *and* $x \equiv 3$ *(impossible).*
7. $x-1 \equiv 4$ *and* $x+4 \equiv 3 \Rightarrow x \equiv 5$ *and* $x \equiv 5$ *(possible).*
8. $x-1 \equiv 3$ *and* $x+4 \equiv 4 \Rightarrow x \equiv 4$ *and* $x \equiv 0$ *(impossible).*

From this analysis, we conclude that the possible solutions in $\mathbb{Z}_6$ *are* $x \equiv 1, 2, 4$ *(more than two ☺).*

Exercise 37 *Consider a ring* R *with more than one element. Given that for every* $a \in R$*, there exists a unique* $b \in R$ *such that* $aba = a$*. Then prove that:*

1. $bab = b$.
2. *R is a division ring.*

Proposition .24 *Any finite field* F *must have a prime power order.*

Hint(s): *If there exist distinct primes* p *and* q $(p < q)$ *such that* $p, q \mid |F|$*, then* F *will have zero divisors. Suppose* $O(a) = p$ *and* $O(b) = q$ *(additive orders). Then,* $a(pb) = (ap)b = 0.b = 0$*, but* $a \neq 0$ *and* $pb \neq 0$*.*

Exercise 38 *Does there exist an integral domain with 6 elements?*

Exercise 39 1. *If in* R*,* $x^2 = x$ *for all* $x \in R$*, then* R *is a commutative ring with characteristic* $= 2$*.*

2. *If* $x^3 = x$ *for all* $x \in R$*, then* R *is a commutative ring.*

1.12. Subrings and Ideals

Definition .47 (Subring) *A non-empty subset* S *of* $(R, +, *)$ *is called a subring of* R *if and only if* $(S, +, *)$ *is itself a ring.*

Theorem .32 *Let* $S \subseteq R$*, where* R *is a ring. Then,* S *is a subring if and only if* $\forall\ a, b \in S$*:*

1. $a - b \in S$
2. $ab \in S$

Example 1.12.1 1. $\mathbb{Z}$ *is a subring of* $\mathbb{Q}$*.*

2. $n\mathbb{Z}$ *is a subring of* $\mathbb{Z}$*.*
3. $R_1 = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R}\right\}$ *is a subring of* $R_2 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R}\right\}$*.*
4. $\mathbb{Z} \times \{0\} = \{(a, 0) : a \in \mathbb{Z}\}$ *is a subring of* $\mathbb{Z} \times \mathbb{Z}$*.*

Remark 4 *In the above four examples, it is worth noting that:*

1. *A ring and its subring share the same identity (unity).*
2. *A ring has a unity, but a subring does not.*
3. *A ring has no identity, but a subring has* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$*.*
4. *A ring and its subring both have an identity, but they are different; the identity of the ring is* $(1, 1)$ *and the identity of the subring is* $(1, 0)$*.*

Exercise 40 *The arbitrary intersection of subrings is again a subring of the given ring R.*

Exercise 41 *The union of subrings may not be a subring.*

Hint(s): *$2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings of $\mathbb{Z}$, but $2\mathbb{Z}\cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$ as $2\in\mathbb{Z}$, $3\in\mathbb{Z}$, but $2+3=5\notin 2\mathbb{Z}\cup 3\mathbb{Z}$.*

Proposition .25 *The sum of two subrings of a ring R need not be a subring of R.*

Hint(s): *Try with $R_1=\left\{\begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix} : a\in\mathbb{Z}\right\}$ and $R_2=\left\{\begin{pmatrix}0 & 0\\ b & 0\end{pmatrix} : b\in\mathbb{Z}\right\}$. Their sum is not closed under multiplication.*

Definition .48 (Center of a Ring) *The center of a ring $C(R)=\{a\in R : xa=ax\ \forall\ x\in R\}$ is a subring of R.*

Exercise 42 *R is commutative if and only if $C(R)=R$.*

Exercise 43 *Prove that the center $C(R)$ of a division ring R is a field.*

1.13. Ideals

Definition .49 *Let R be a ring and I be a subring of R.*

1. *If $\forall\ r\in R$ and $a\in I$, then $ra\in I$. I is called a left ideal of R ($rI\subseteq I$).*
2. *If $\forall\ r\in R$ and $a\in I$, then $ar\in I$. I is called a right ideal of R ($Ir\subseteq I$).*

If I is a two-sided ideal, we simply say it is an ideal. In a commutative ring, all ideals are two-sided.

Exercise 44 *Is $\mathbb{Z}$ an ideal of $\mathbb{Q}$? (It is already known that it is a subring.)*

Remark 5 *In general, an ideal $\Rightarrow$ subring, but subring $\not\Rightarrow$ ideal.*

Example 1.13.1 *Show that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n\in\mathbb{N}$.*

Solution: *Let $a\in n\mathbb{Z}$ and $r\in\mathbb{Z}$. Here $a=nx$, $x\in\mathbb{Z}$. Therefore, $ar=(nx)r=n(xr)=nx'\in n\mathbb{Z}$. Also, for all $a,b\in n\mathbb{Z}$, $a-b=nx-ny=n(x-y)\in n\mathbb{Z}$. Hence, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.*

Exercise 45 *The intersection of a family of left (right) ideals is also a left (right) ideal.*

Definition .50 *Let S be any subset of a ring R, then the ideal I is said to be generated by S if*

1. *$S\subseteq I$*
2. *For any ideal J of S such that $S\subseteq J$, $I\subseteq J$; in other words, I is the smallest.*

I is the smallest ideal of R containing S, denoted as $I=\langle S\rangle$.

$$I=\bigcap\{J : S\subseteq R \text{ and } J \text{ is an ideal}\}$$

1.14. Principal Ideal

Definition .51 *An ideal generated by a single element is called a principal ideal of the ring.*

Example 1.14.1

1. *$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, which is a principal ideal, i.e., $n\mathbb{Z}=\langle n\rangle$.*
2. *Let R be a commutative ring with unity. Then $\forall\ a\in R$, $aR=\{ar : r\in R\}=\langle a\rangle$ is a principal ideal.*

Definition .52 *Let I and J be two ideals of a ring R, then the sum $I+J=\{a+b : a\in I, b\in J\}$ and the product $IJ=\{\sum_{i=1}^{n}a_ib_i : a_i\in I, b_i\in J, n\in\mathbb{N}\}$.*

Exercise 46

1. *Prove that $I+J$ is an ideal given by $I+J=\langle I\cup J\rangle$, which is the smallest ideal of R containing $I\cup J$.*
2. *Prove that IJ is also an ideal and $IJ\subseteq I\cap J$.*

Hint(s): *1. Let I and J be ideals of a ring R.* ***Step 1:*** *$I+J$ is an ideal: - Closure under addition and multiplication by elements of R follows from I and J being ideals.* ***Step 2:*** *$I+J \subseteq \langle I\cup J\rangle$: - For any $x\in I+J$, $x=a+b$ with $a\in I$ and $b\in J$. Since $I\subseteq\langle I\cup J\rangle$ and $J\subseteq\langle I\cup J\rangle$, $x\in\langle I\cup J\rangle$.* ***Step 3:*** *$\langle I\cup J\rangle$ is an ideal: - Follows from properties of generated ideals.* ***Step 4:*** *$\langle I\cup J\rangle\subseteq I+J$: - Since $\langle I\cup J\rangle$ contains elements from I and J, it also contains their sums, which are in $I+J$.*
2. Let I and J be ideals of a ring R. ***Step 1:*** *IJ is an ideal: - Closure under addition and multiplication by elements of R follows from the properties of I and J.* ***Step 2:*** *$IJ\subseteq I\cap J$: - Take any $x\in IJ$, then $x=\sum_{i=1}^{n}a_ib_i$ for $a_i\in I$ and $b_i\in J$. - Since $a_i\in I$ and $b_i\in J$, $x\in I\cap J$. Thus, IJ is an ideal and $IJ\subseteq I\cap J$.*

Exercise 47 *If $I=\langle a\rangle$, $J=\langle b\rangle$, then find $I+J$, IJ, and $I\cap J$, where $a,b\in\mathbb{Z}^+$.*

Answers: *$I+J=U$, where $U=\langle d\rangle$ with $d=gcd\{a,b\}$. $I\cap J=V$, where $V=\langle c\rangle$ with $c=lcm\{a,b\}$. $IJ=W$, where $W=\langle ab\rangle$.*
Solution: *Given $I=\langle a\rangle$, $J=\langle b\rangle$, we have:*

1. *$d=gcd(a,b)$, i.e., $d|a$, $d|b$, which means $a=n_1d$, $b=n_2d$. Thus, $a\in\langle d\rangle$, $b\in\langle d\rangle$, implying $\langle a\rangle\subseteq\langle d\rangle$, $\langle b\rangle\subseteq\langle d\rangle$. Hence, $\langle a\rangle+\langle b\rangle\subseteq\langle d\rangle$. Also, there exist integers x and y such that $d=ax+by$. This implies $\langle d\rangle\subseteq\langle a\rangle+\langle b\rangle$. Thus, $\langle d\rangle=\langle a\rangle+\langle b\rangle$.*

2. *Let $c=lcm(a,b)$, i.e., $a|c$, $b|c$. This means $\langle c\rangle\subseteq\langle a\rangle$, $\langle c\rangle\subseteq\langle b\rangle$, hence $\langle c\rangle\subseteq\langle a\rangle\cap\langle b\rangle$. Also, if $x\in\langle a\rangle\cap\langle b\rangle$, then $a|x$, $b|x$. Consequently, $lcm(a,b)|x$, i.e., $c|x$, which leads to $x\in\langle c\rangle$. Therefore, $\langle a\rangle\cap\langle b\rangle=\langle c\rangle$.*

3. *$a\in\langle a\rangle$, $b\in\langle b\rangle$, so $ab\in\langle a\rangle\langle b\rangle$, i.e., $\langle ab\rangle\subseteq\langle a\rangle\langle b\rangle$. Let $x\in\langle a\rangle\langle b\rangle$. Then $x=\sum_{finite\ sum}a_ib_i$, where $a_i\in\langle a\rangle$ and $b_i\in\langle b\rangle$. Observe that $a_ib_i=(ak_i)(bk_i')=(k_ik_i')(ab)$, implying $a_ib_i\in\langle ab\rangle$. Hence, $x\in\langle ab\rangle$. Therefore, $\langle ab\rangle=\langle a\rangle\langle b\rangle$.*

Definition .53 (Maximal Ideal) *A non-zero ideal $S\neq R$ of a ring R is called a maximal ideal of R if there exists no proper ideal of R containing S.*

Exercise 48 *Prove that $J=\langle 4\rangle$ is a maximal ideal of $E=\langle 2\rangle$.*

Solution: *Since $2\notin\langle 4\rangle$, we have $J\neq E$. Let K be any ideal such that $J\subseteq K$, where $J\neq K$ and $K\subseteq E$. Therefore, there exists some $x\in K$ such that $x\notin J$, implying x is not a multiple of 4. Write $x=4m+r$, where $r=1,2,3$. Analyze cases for r to deduce that $2\notin K$, leading to $K=E$. Thus, $J=\langle 4\rangle$ is a maximal ideal of $E=\langle 2\rangle$.*

Definition .54 (Simple Ring) *If 1. $\exists\ a,b\in R$ such that $ab\neq 0$ 2. R has no proper ideal.*
(or) R is with unity and has no proper ideal.

Example 1.14.2 *Every field is a simple ring. The ideals of a field F are F and $\{0\}$ only.*

Exercise 49 *Show that $\langle\{0,1,2,3,4\},+_5,*_5\rangle$ has no proper ideal.*

Note 22 *$I^2=\{\sum_{finite\ sum}a_ib_i\ :\ a_i,b_i\in I\}$*

Definition .55 (Nilpotent Ideal) *An ideal I of R is called a nilpotent ideal if for some positive integer n, $I^n=\{0\}$.*

Definition .56 (Nil Ideal) *An ideal I of a ring R is said to be a nil ideal if each element of I is nilpotent, i.e., $\forall\ a\in I$, $\exists\ n$ such that $a^n=0$.*

Proposition .26 *Every nilpotent ideal is a nil ideal.*

The converse of the above proposition may not be true (out of scope).

1.15. Factor/Quotient Ring

Definition .57 (Factor/Quotient Ring) *Let I be an ideal of a ring R. Define R/I as the set $\{a+I\ :\ a\in R\}$, with the operations*

$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)(b+I)=ab+I$$

Under this structure, R/I forms a ring.

Exercise 50 *Consider the ideal $I = \{6n : n \in \mathbb{Z}\}$ of the ring $\mathbb{Z}$. Write the multiplication table for $\mathbb{Z}/I$ and determine if $\mathbb{Z}/I$ is an integral domain.*

Theorem .33 *If R is a commutative ring with unity, then R/M is a field if and only if M is a maximal ideal of R.*

Proof: *Let M be a maximal ideal of R. Since R is commutative and has unity, R/M inherits these properties. To prove that every non-zero element in R/M is a unit, let $\bar{x} \in R/M$, represented as $\bar{x} = x + M$ with $x \in R$. Consider the ideal $xR = \{xr : r \in R\}$; it is a subset of R. Since M is a proper subset of xR (due to $0 \neq x$), by the maximality of M, we have $M \neq M + xR = R$. Thus, there exists an $xr \in xR$ such that $xr \in M$ but $xr \notin M$ ($M \subsetneq xR$). This implies that $1 = xr + m$ for some $m \in M$, leading to $\bar{1} = \bar{x}\bar{r}$, making $\bar{x}$ a unit in R/M.*

Conversely, assume R/M is a field. We need to show that M is maximal. Since $1 \notin M$ (otherwise $M = R$), consider the assumption that there exists an ideal I with $M \subset I \subseteq R$. This implies there exists an $a \in I$ such that $a \notin M$, and thus $\bar{a} \neq \bar{0}$. Since R/M is a field, there exists a $\bar{b}$ such that $\bar{a}\bar{b} = \bar{1}$, which leads to $ab + M = 1 + M$ and $(1 - ab) \in M \subseteq I$. As $a \in I$ and $b \in R$, we get $ab \in I$, so $1 \in I$, which ultimately means $I = R$. Therefore, M is a maximal ideal.

Exercise 51

1. *Prove that in $\mathbb{Z}$, $n\mathbb{Z}$ is maximal if and only if n is prime.*
2. *Verify that $M = \{0, 3, 6, 9\}$ is a maximal ideal of $\mathbb{Z}_{12}$.*
   Hint(s): *Order of $\frac{\mathbb{Z}_{12}}{M}$ is $|\frac{\mathbb{Z}_{12}}{M}| = \frac{12}{4} = 3$, and $\frac{\mathbb{Z}_{12}}{M} = \{\bar{0}, \bar{1}, \bar{2}\}$ is an integral domain and so a field. Since $\frac{\mathbb{Z}_{12}}{M}$ is a field, M is a maximal ideal of $\mathbb{Z}_{12}$.*

Definition .58 (Prime Ideal) *Let R be a commutative ring. An ideal P of R is called a prime ideal if for all $a, b \in R$, whenever $ab \in P$, it follows that either $a \in P$ or $b \in P$.*

Example 1.15.1

1. *If R is an integral domain, then $< 0 >$ is a prime ideal of R because $ab \in < 0 >$ implies $ab = 0$, which leads to either $a = 0$ or $b = 0$. Hence, either $a \in < 0 >$ or $b \in < 0 >$.*
2. *In $\mathbb{Z}$, $I = < 3 >$ is a prime ideal. If $ab \in I$, then $ab = 3n \Rightarrow 3|ab \Rightarrow 3|a$ or $3|b \Rightarrow a = 3m_1$ or $b = 3m_2 \Rightarrow a \in < 3 >$ or $b \in < 3 > \Rightarrow I$ is a prime ideal.*

Proposition .27 *The quotient ring R/M is an integral domain if and only if M is a prime ideal, where R is a commutative ring with unity.*

Proof: *Assume R/M is an integral domain. If $ab \in M$, then $\bar{a}\bar{b} = \bar{0}$ in R/M. Since R/M is an integral domain, $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. This implies $a \in M$ or $b \in M$.*

Conversely, suppose M is a prime ideal. If $\bar{a}.\bar{b} = \bar{0}$ in R/M, then $ab \in M$, leading to $a \in M$ or $b \in M$. This implies $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ in R/M, confirming that R/M is an integral domain.

Note 23 *If R is a commutative ring with unity, then R/M is also a commutative ring with unity.*

Corollary .34 *Every maximal ideal is a prime ideal.*

Proof: *A maximal ideal M corresponds to a field R/M. Since a field is an integral domain, M is a prime ideal.*

Remark 6 *The converse of the above result is not always true. For example, $< 0 >$ is a prime ideal but not maximal in $\mathbb{Z}$, as $< 2 >$ is an ideal with $< 0 > \subset < 2 > \subset \mathbb{Z}$.*

Example 1.15.2 *Consider $R = \mathbb{Z} \times \mathbb{Z}$, which is a ring where a prime ideal is not necessarily maximal.*

Solution: *Let $R = \mathbb{Z} \times \mathbb{Z}$ and $I = < (1, 0) >$. Now, I is a prime ideal. Let $X = (a_1, b_1)$ and $Y = (a_2, b_2)$ for $x, y \in \mathbb{R}$, and note that $XY = (a_1a_2, b_1b_2) \in I$. As $\mathbb{Z}$ is an integral domain, $b_1b_2 = 0$, implying $b_1 = 0$ or $b_2 = 0$. This leads to $X = (a_1, 0) \in I$ or $Y = (a_2, 0) \in I$. However, there exists $J = \{(a, 2b) : a, b \in \mathbb{Z}\} = < (1, 0), (0, 2) >$ such that $I \subset J \subset R$. Thus, I is not maximal, but it is prime.*

Example 1.15.3 *Consider $R = 2\mathbb{Z}$. The ideal $< 4 >$ is a maximal ideal but not prime, as $2 \cdot 6 \in < 4 >$ but $2 \notin < 4 >$ and $6 \notin < 4 >$. (Why? Since R is without unity).*

Proposition .28 *If R is a finite ring, then every prime ideal is also a maximal ideal.*

Hint(s): *A ring is a field if the ring is a finite integral domain.*

Exercise 52 *Determine all prime ideals and maximal ideals of* $\mathbb{Z}_8$.

Exercise 53 *Prove that* $<x>$ *is a prime ideal of* $\mathbb{Z}[x]$*, but it is not maximal. Here,* $\mathbb{Z}[x] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in \mathbb{Z}, n \in \mathbb{N}\}$ *is the ring of polynomials.*

Hint(s): *If* $f(x)g(x) \in <x>$*, then* $f(0)g(0) = 0$*. Both* $f(0)$ *and* $g(0)$ *are in* $\mathbb{Z}$ *(which is an integral domain). This implies* $f(0) = 0$ *or* $g(0) = 0$*, leading to* $f(x) \in <x>$ *or* $g(x) \in <x>$*. Moreover, we have* $<x> \subseteq <x,2> \subseteq \mathbb{Z}[x]$.

1.16. The Field of Quotients of an Integral Domain

Similar to how the ring of integers can be extended to include the set of rational numbers, we can perform a similar extension for any integral domain.

Definition .59 *A ring* R *can be embedded in a ring* R' *if there exists an injective ring homomorphism from* R *to* R'.

R' *is called an extension of* R *if* R *can be embedded in* R'.

Theorem .35 *Every integral domain can be embedded in a field, which means we can extend an integral domain to a field.*

Proof: *Let* D *be an integral domain. Consider all quotients* a/b *where* $a \in D$ *and* $b \neq 0$ *in* D*. We denote* a/b *(which has no defined meaning in* D*) as* (a,b)*. Define a relation* $\sim$ *such that* $(a,b) \sim (c,d)$ *if and only if* $ad = bc$*. This relation is an equivalence relation, and we use the equivalence class containing* (a,b) *to denote the set* $[a,b]$*. We claim that* F*, defined as the set of all these equivalence classes, serves as our desired extension field.*

Additionally, we define addition and multiplication on F *as follows:*

$$[a_1,b_1] + [a_2,b_2] = [a_1b_2 + b_1a_2, b_1b_2]$$
$$[a_1,b_1] \cdot [a_2,b_2] = [a_1a_2, b_1b_2]$$

where $b_1b_2 \neq 0$.

Exercise 54 *For the structure defined in the proof above, prove all the properties of a field.*

Hint(s): $[0,b]$ *serves as the additive identity,* $[-a,b]$ *is an additive inverse,* $[c,d]^{-1} = [d,c]$ *etc.*

F *is often referred to as the field of fractions, in the specific case where* $D = \mathbb{Z}$*,* $F = \mathbb{Q}$.

1.17. Euclidean Rings

Definition .60 *An integral domain* R *is termed a Euclidean ring if, for all* $0 \neq a \in R$*, there exists a non-negative integer* $d(a)$ *satisfying the following conditions:*

1. $d(a) \leq d(ab)$
2. *For all* $0 \neq a, 0 \neq b \in R$*, there exist* $t, r \in R$ *such that* $a = tb + r$*, where* $r = 0$ *or* $d(r) < d(b)$.

There is no assigned value for $d(0)$.

Example 1.17.1 *The ring* $R = \mathbb{Z}$ *is a Euclidean ring, with* $d(a) = |a|$*, satisfying the following:*

1. $|a| \leq |ab|$ *for all* $a, b \in \mathbb{Z}$ *where* $a \neq 0$ *and* $b \neq 0$
2. *For any* $a, b \in \mathbb{Z}$ *where* $a \neq 0$ *and* $b \neq 0$*, we have* $a = tb + r$ *with* $r = 0$ *or* $|r| < |b|$.

Definition .61 *An integral domain* R *with unity is a principal ideal ring if every ideal of* R *is of the form* $<a>$ *for some* $a \in R$.

Theorem .36 *Every Euclidean ring (domain) is a principal ideal ring (domain).*

[Euclidean Domain $\Rightarrow$ *Principal Ideal Domain]*

Proof: *If* $A = \{0\}$*, then* $A = <0>$*, where* A *is an ideal of an Euclidean domain. Suppose* $A \neq \{0\}$*, and let* $a_0 \in A$ *such that* $d(a_0)$ *is minimal. Now, if* $a \in A$*, then there exist* $t, r \in R$ *such that* $a = ta_0 + r$ *with* $r = 0$ *or* $d(r) < d(a_0)$*. Also, since* $a \in A$ *and* $a_0 \in A$*, we have* $ta_0 \in A$*, which is an ideal. This implies* $a - ta_0 \in A$*, and therefore,* $r \in A$ *with*

$d(r) < d(a_0)$, leading to a contradiction. Hence, $r = 0$, which means $a = ta_0$, and thus $A =< a_0 >$, proving that it is a principal ideal.

Corollary .37 *An Euclidean ring possesses unity.*

Proof: *Let R be an Euclidean ring. By the previous theorem, $R =< a_0 >$ for some $a_0 \in R$, and $a_0 = a_0 c$ for some c. Consider any arbitrary $a \in R$. Then, $a = xa_0$, and hence $ac = xa_0 c = xa_0 = a$, which implies $ac = a$. This means c serves as the unity.*

Note 24 *Why do we need this result? An integral domain already possesses a unity. This means that if you consider the definition of an integral domain without unity, a Euclidean ring will still automatically possess unity.*

If $a \neq 0$ and b are elements of the ring R, then a is said to divide b if there exists $c \in R$ such that $b = ac$. We write $a|b$ to represent that a divides b, and $a \nmid b$ indicates that a does not divide b.

Definition .62 (Greatest Common Divisor) *If $a, b \in R$, then $d \in R$ is said to be the greatest common divisor of a and b if:*

1. *$d|a$ and $d|b$*
2. *Whenever $c|a$ and $c|b$, then $c|d$ for any $c \in R$.*

We denote d as (a, b), which is the gcd of a and b.

Theorem .38 *Let R be an Euclidean ring. Then any two elements a and b in R have a gcd d. Moreover, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.*

Proof: *Let $a, b \in R$. Define a set $A = \{ra + sb \ : \ r, s \in R\}$. It can be proven that A is an ideal of R, and R being an Euclidean ring is also a principal ideal domain. Thus, $A =< d >$ for some $d \in R$, implying $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. Furthermore, $1 \in R$, so $a = a \cdot 1 + b \cdot 0 \in A$ and $b = b \cdot 1 + a \cdot 0 \in A$, given that $a, b \in A =< d >$. This yields $a = dc_1$ and $b = dc_2$ for some $c_1, c_2 \in R$, resulting in $d|a$ and $d|b$. Moreover, if $c|a$ and $c|b$, then $c|(\lambda a + \mu b) = d$, which establishes $c|d$. Hence, the result follows.*

In an integral domain, if $a|b$ and $b|a$, then $a = \mu b$ where μ is a unit.

Definition .63 (Associates) *Two elements $a, b \in R$ are said to be associates if $a = \mu b$ for some $\mu \in R$.*

Definition .64 (Irreducible element) *Let R be a Euclidean ring. An element (non-unit) r is said to be irreducible if whenever $r = ab$ for some $a, b \in R$, either a is a unit or b is a unit in R.*

An element is reducible if it is not irreducible.

Theorem .39 *Every reducible element in R (Euclidean ring) can be expressed as a product of irreducible elements in R.*

Proof: *Let $a \in R$ be reducible, i.e., $a = bc$ where neither b nor c is a unit. We have $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Using induction, $b = r_1 r_2 \cdots r_n$ and $c = r'_1 r'_2 \cdots r'_n$, so $a = r_1 r_2 \cdots r_n r'_1 r'_2 \cdots r'_n$. Thus, the theorem is proved.*

1.18. Unique Factorization Theorem

Theorem .40 *An ideal $A =< a_0 >$ is a maximal ideal in the Euclidean ring R if and only if a_0 is an irreducible element of R.*

Proof: *Suppose $a_0 = bc$, where neither b nor c is a unit. Let $B =< b > \Rightarrow a_0 \in B \Rightarrow A \subseteq B$.*

1. *If $B = R$, then $1 = xb$, which implies that b is a unit, leading to a contradiction.*
2. *If $A = B$, then $b \in A \Rightarrow b = xa_0$. Also, since $a_0 = bc$, we have $a_0 = xca_0 \Rightarrow 1 = xc$, which makes c a unit. Hence, a_0 is not an irreducible element, which contradicts the assumption. Therefore, if A is a maximal ideal, then a_0 must be irreducible.*

Conversely, if there exists a set U such that $A \subset U \subset R$, let $A =< a_0 >$ and $U =< d_0 >$. Since R is a principal ideal domain (Euclidean domain $\Rightarrow$ Principal ideal domain), we have $a_0 \in A \subset U \Rightarrow a_0 \in< d_0 >$. This implies that $a_0 = d_0 x$, *but since a_0 is irreducible by assumption, either d_0 or x must be a unit.*

1. *If d_0 is a unit, then a unit is in U, which means $U = R$ (since $1 \in U$).*
2. *If x is a unit, then $d_0 = x^{-1}a_0 \in A$ (ideal), where $x^{-1} \in R$, implying that $a_0 \in A$. This means $U \subset A$, and since $A \subset U$, we conclude that $A = U$, making A a maximal ideal.*

Corollary .41 *In a principal ideal domain, irreducible elements are also prime elements.*

Hint(s): *maximal ideal $\Rightarrow$ prime ideal.*

Theorem .42 *Let R be a Euclidean ring. If $a \neq 0$ is a non-unit in R, and $a = r_1 r_2 \cdots r_n = r'_1 r'_2 \cdots r'_m$ where r'_i, r_i are irreducible elements in R, then $n = m$ and r_i is associated with r'_j for some i, j.*

Proof: *Since $r_1 | r'_1 r'_2 \cdots r'_m \Rightarrow r_1 | r'_i$ for some i. Therefore, $r'_i = r_1 u_1$, where u_1 is a unit in R, since r_1 and r'_i are irreducible elements. This implies $r_1 r_2 \cdots r_n = r'_1 r'_2 \cdots (r_1 u_1) r'_{i+1} \cdots r'_m \Rightarrow r_2 \cdots r_n = (r'_2 \cdots r'_m) u_1$. Repeat this process until we get $1 = (r'_{n+1} \cdots r'_m) u_1 u_2 \cdots u_n$. Since r'_i are not units, we have $n \leq m$. Without loss of generality, assume $m \leq n$, yielding $m = n$. From the previous result, we can conclude that r_i is associated with some r'_j, where $1 \leq i \leq n$ and $1 \leq j \leq m$.*

Definition .65 (Unique Factorization Domain) *A ring R is a unique factorization domain if R is an integral domain and every non-zero element of R can be expressed uniquely as a product of a finite number of irreducible elements (up to associates).*

Example 1.18.1

1. *$\mathbb{Z}$ is a unique factorization domain.*
2. *Every principal ideal domain is a unique factorization domain.*
3. *Every field is a unique factorization domain.*
4. *Every Euclidean domain is a unique factorization domain.*

Exercise 55 *Every principal ideal domain is a unique factorization domain.*

Hint(s): *Let $a \in D$ (principal ideal domain). Then $a = r_1 a_1$, where r_1 is irreducible and $(a_1) \supset (a)$. Similarly, $a_1 = r_2 a_2 \Rightarrow (a_2) \supset (a_1)$, and so on. This gives rise to a chain $(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$. Since $I_n = \bigcup_{n=1}^{\infty} (a_n)$ is a principal ideal, we have $I_\infty =< b >$, where $b \in< a_n >$ for some n. In other words, $< b >\subseteq< a_n >$, which proves that the factorization is irreducible. Additionally, in a principal ideal domain, every irreducible element implies a prime element, making the factorization unique.*

Proposition .29 *$\mathbb{Z}[i]$ is a Euclidean ring.*

Proof: *Define a function*

$$d : \mathbb{Z}[i] \to \mathbb{Z}^+ \cup \{0\}$$
$$d(x) = a + ib \mapsto a^2 + b^2 \text{ for all } x = a + ib \in \mathbb{Z}[i]$$

1. *Clearly, $d(x) \geq 0$ for all $x \in \mathbb{Z}[i]$ and is a non-negative integer function. Furthermore, $d(y) \geq 1$ for all $y \in \mathbb{Z}[i]$.*
2. *$d(x) = d(x) \cdot 1 \leq d(x) \cdot d(y) = d(xy)$ (since $d(xy) = d(x)d(y)$ for all $x, y \in \mathbb{Z}[i]$).*
3. *For a specific case: Let x be a positive integer and $y \in \mathbb{Z}[i]$. Use the division algorithm: $\exists u, v \in \mathbb{Z}$ such that $a = un + u_1$ and $b = vn + v_1$, where $|u_1| \leq \frac{1}{2}n$ and $|v_1| \leq \frac{1}{2}n$ for all $n \in \mathbb{Z}$. Let $t = u + iv$ and $r = u_1 + iv_1$. Then $y = tx + r_1$. Since $d(r) = d(u_1 + iv_1) = u_1^2 + v_1^2 \leq \frac{1}{4}n^2 + \frac{1}{4}n^2 = \frac{n^2}{2} \leq n^2 = d(n)$, we have $y = tx + r$ with $r = 0$ or $d(r) < d(n)$.*

Note 25 *$a \sim b \Leftrightarrow < a >=< b >$*

Proposition .30 *In an integral domain, a prime element implies an irreducible element.*

Proof: *Let $p = ab$, where p is prime. Then $I =< p >$ is a prime ideal, which implies that $ab \in I \Rightarrow a \in I$ or $b \in I$. This means $a = px$ or $b = py$. If $a = px$, then $p = pxb \Rightarrow 1 = xb$, making b a unit. Similarly, $b = py$ implies a is a unit. Therefore, p is irreducible.*

Exercise 56 *In a unique factorization domain, every irreducible element is a prime element.*

Hint(s): *Assume p is an irreducible element in a UFD R. To show that p is prime, consider $a, b \in R$ such that p divides $a \cdot b$. Since p is irreducible, it cannot be further factored. Therefore, the factorization of $a \cdot b$ involves p.*

Now, suppose p does not divide a. Since p is irreducible and it divides $a \cdot b$, it must divide b (otherwise the factorization of $a \cdot b$ wouldn't involve p). This implies that p divides b, making it a divisor of both a and b. Thus, p is shown to be a prime element in the UFD R.

Example 1.18.2 *$\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain, as $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$, where 3 is not an associate of $2+\sqrt{-5}$ or $2-\sqrt{-5}$.*

Solution: *Suppose for contradiction that 3 is an associate of $2+\sqrt{-5}$ or $2-\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. This implies there exists a unit u such that $3 = u \cdot (2+\sqrt{-5})$ or $3 = u \cdot (2-\sqrt{-5})$.*

Now, take the norm of both sides of the equation. The norm is multiplicative, so $N(3) = N(u)N(2+\sqrt{-5})$ or $N(3) = N(u)N(2-\sqrt{-5})$. But the norm of 3 is 9, and the norms of $2+\sqrt{-5}$ and $2-\sqrt{-5}$ are also 9.

Hence, $9 = N(u) \cdot 9$. This implies that $N(u) = 1$. However, the only units in $\mathbb{Z}[\sqrt{-5}]$ with norm 1 are 1 and -1. Since u is a unit, this leads to a contradiction.

Proposition .31 *In a unique factorization domain, every pair of elements has a highest common factor (HCF) and a lowest common multiple (LCM).*

Proposition .32 *If R is a ring with unity and the characteristic of R is n, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.*

Hint(s): *Define $\phi : \mathbb{Z} \to S = \{k \cdot 1 : k \in \mathbb{Z}\} \subseteq R$ as $\phi(k) = k \cdot 1$ for all $k \in \mathbb{Z}$. Then $\frac{\mathbb{Z}}{\ker\phi} \simeq S$ (ϕ is onto and a homomorphism). Here, $\ker\phi = \{x \in \mathbb{Z} : \phi(x) = 0\}$.*

1. *$\ker\phi = \mathbb{Z}_n$ if char(R) = n*
2. *$\ker\phi = \{0\}$ if char(R) = 0*

Thus, $\mathbb{Z}_n \simeq S \subset R$ or $\mathbb{Z} \simeq S \subseteq R$.

Proposition .33 *$\mathbb{Z}_m$ is a homomorphic image of $\mathbb{Z}$.*

Hint(s): *Define $\phi : \mathbb{Z} \to \mathbb{Z}_m$ by $\phi(x) = x \ (mod\ m)$.*

Proposition .34 *A field F contains either $\mathbb{Q}$ or $\mathbb{Z}_p$.*

Hint(s):

1. *If char(F) = p, then F contains a subfield isomorphic to $\mathbb{Z}_p$.*
2. *If char(F) = 0, then F contains a subfield isomorphic to $\mathbb{Q}$.*

Example 1.18.3 *Prove that 3 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$.*

Solution: *Assume that $3 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \Rightarrow 9 = (a^2+5b^2)(c^2+5d^2)$.*

1. *$a^2+5b^2 = 1$ and $c^2+5d^2 = 9$. This has a solution if $a = \pm 1$ and $b = 0$.*
2. *$a^2+5b^2 = 3$ and $c^2+5d^2 = 3$. This has no solution.*
3. *$a^2+5b^2 = 9$ and $c^2+5d^2 = 1$. This has a solution if $c = \pm 1$ and $d = 0$.*

$\Rightarrow (a+\sqrt{-5}b) = \pm 1$ or $(c+\sqrt{-5}d) = \pm 1$ are units of $\mathbb{Z}[\sqrt{-5}] \Rightarrow 3$ is irreducible.
However, $3 | 9 = (2+\sqrt{-5})(2-\sqrt{-5})$, and 3 is not an associate of $2+\sqrt{-5}$ or $2-\sqrt{-5}$. Therefore, 3 is not a prime element.

Note 26 *In general, prime numbers are not always prime elements.*

Exercise 57 *Prove that $1+i$ is an irreducible element in $\mathbb{Z}[i]$.*

Hint(s): *Assume, for contradiction, that $1+i$ is not irreducible in $\mathbb{Z}[i]$. This implies that it can be factored as $1+i=(a+bi)(c+di)$, where $a+bi$ and $c+di$ are non-unit elements in $\mathbb{Z}[i]$.*

Expanding and simplifying, we get $1+i=(ac-bd)+(ad+bc)i$. Equating real and imaginary parts, we have $ac-bd=1$ and $ad+bc=1$.

Adding the squares of these equations, we get $(a^2+b^2)(c^2+d^2)=2$, which is a contradiction since the left side is a non-negative integer. Hence, the assumption is false, and $1+i$ is indeed irreducible in $\mathbb{Z}[i]$.

Example 1.18.4 *In $\mathbb{Z}_6$, $\bar{2}$ is prime but not irreducible.*

Hint(s): *$\bar{2}|\bar{a}\bar{b} \Rightarrow 2|ab \Rightarrow 2|a$ or $2|b \Rightarrow \bar{2}|\bar{a}$ or $\bar{2}|\bar{b}$. Here, $\bar{a}\bar{b}=ab+2k$, but $\bar{2}=\bar{2}\cdot\bar{4}$, and neither $\bar{2}$ nor $\bar{4}$ is a unit. Therefore, $\bar{2}$ is not an irreducible element. Thus, $\mathbb{Z}_6$ is not an integral domain.*

Remark 7 *In an integral domain, prime elements are also irreducible elements.*

Example 1.18.5
1. *Every field is a principal ideal domain.*
2. *$\mathbb{Z}$ is a principal ideal domain.*

Example 1.18.6 *Consider $\mathbb{Z}_{12}$. The element $\bar{2}$ is the highest common factor (HCF) of $\bar{6}$ and $\bar{8}$. We claim that $\bar{10}$ is also an HCF (not unique).*

Hint(s): *$\bar{6}=\bar{3}\bar{2}$, $\bar{8}=\bar{4}\bar{2}$. If $\bar{x}|\bar{6}$ and $\bar{8}$, then $\bar{x}|(\bar{8}-\bar{6})=\bar{2}$. Now, $\bar{6}=\bar{10}\bar{3}$ and $\bar{8}=\bar{10}\bar{2}$. If $\bar{y}|\bar{6}$ and $\bar{8}$, then $\bar{y}|(\bar{2}\bar{8}-\bar{6})=\bar{10}$. It's clear that $\bar{2}|\bar{10}$ and $\bar{10}|\bar{2}$.*

Moreover, the least common multiple (LCM) of $\bar{6}$ and $\bar{8}$ does not exist. If $\bar{6}|\bar{x}$ and $\bar{8}|\bar{x}$, then $\bar{x}=\bar{6}\bar{n}$ implies $\bar{x}=\bar{0},\bar{6}$, and $\bar{x}=\bar{8}\bar{m}$ implies $\bar{x}=\bar{0},\bar{4},\bar{8}$. Therefore, $\bar{x}=\bar{0}$ is the only common choice, which is impossible. Hence, the LCM does not exist.

Proposition .35 *In a principal ideal domain, every non-zero pair a and b has the highest common factor (HCF) and the least common multiple (LCM).*

Proposition .36 *Two elements are coprime if their highest common factor (HCF) is a unit.*

1.19. Polynomial Rings

Definition .66 *Let R be a commutative ring. The set $R[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in R\}$ is called the ring of polynomials over R.*

Exercise 58 *Prove that $R[x]$ is a ring with the usual addition and multiplication of polynomials.*

Theorem .43 *If R is an integral domain, then $R[x]$ is also an integral domain.*

Proof: *$R[x]$ is a ring and is clearly commutative if R is. The element $f=1$ serves as the unit in $R[x]$. Now, let's assume $f(x)\cdot g(x)=0$, where f_n and g_m are the leading coefficients of f and g. This implies $f_ng_m=0$, but since $f_n\neq 0$ and $g_m\neq 0$ (as $f_n, g_m\in R$, which is an integral domain), this leads to a contradiction.*

Theorem .44 *If R is a field, then $R[x]$ is a principal ideal domain.*

Proof: *Consider an ideal I of $R[x]$ (since R is a field, $R[x]$ is an integral domain). Suppose $I\neq<0>$, let $g(x)$ be a polynomial of minimum degree in I. Then $<g(x)>\subseteq I$. Let $f(x)\in I$. By the division algorithm, $f(x)=q(x)g(x)+r(x)$ where $r(x)=0$ or $deg(r(x))<deg(g(x))$, implying $r(x)=f(x)-q(x)g(x)\in I$. If $r(x)$ has a degree less than $g(x)$, then $r(x)=0$, meaning $f(x)\in<g(x)>$, and so $I\subseteq<g(x)>$. This implies $I=<g(x)>$. Thus, $R[x]$ is a principal ideal domain.*

Definition .67 *A polynomial $p(x)$ in $F[x]$ is said to be irreducible over F if, whenever $p(x)=a(x)b(x)$, then one of $a(x)$ or $b(x)$ has degree 0, i.e., it is a constant polynomial.*

Note 27 *Irreducibility depends on the field F.*

Example 1.19.1 *While $x^2+1=(x+i)(x-i)\in\mathbb{C}[x]$, the polynomial x^2+1 is irreducible in $\mathbb{R}[x]$.*

Exercise 59 *Prove that $A=<p(x)>$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible.*

Definition .68 *The polynomial* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *where* a_i*'s are integers is said to be primitive if the greatest common divisor of the* a_i*'s is* 1.

Theorem .45 *If* $f(x)$ *and* $g(x)$ *are primitive polynomials, then* $f(x)g(x)$ *is also a primitive polynomial.*

Proof: *Let* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *and* $g(x) = b_0 + b_1x + \cdots + b_mx^m$. *Suppose* $f(x)g(x)$ *is not primitive, i.e., there exists a prime* p *dividing all coefficients of* $f(x)g(x)$.
Let a_j *be the first coefficient of* $f(x)$ *such that* $p \nmid a_j$ *(since* $f(x)$ *is primitive).*
Similarly, let b_k *be the first coefficient of* $g(x)$ *such that* $p \nmid b_k$. *Consider the coefficient of* x^{j+k}, *denoted as* c_{j+k}. *This coefficient can be expressed as* $c_{j+k} = a_jb_k + (\text{terms divisible by } p)$. *Since* p *does not divide* a_j *and* b_k, *this leads to a contradiction, implying that* $f(x)g(x)$ *is also primitive.*

Definition .69 *The greatest common divisor of all coefficients of* $f(x)$ *(with integer coefficients) is called the content of* $f(x)$.

Theorem .46 (Gauss's Lemma) *If a primitive polynomial* $f(x)$ *can be factored as the product of two polynomials with rational coefficients, it can also be factored as the product of two polynomials with integer coefficients.*

Proof: *Assume* $f(x) = u(x)v(x)$, *where* $u(x)$ *and* $v(x)$ *have rational coefficients. Write* $f(x) = \frac{a}{b}\lambda(x)\mu(x)$, *clearing the denominators, where* a *and* b *are integers. Since* $\lambda(x)$ *and* $\mu(x)$ *are primitive,* $\lambda(x)\mu(x)$ *is also primitive. Therefore,* a *must be equal to* b, *i.e.,* $\frac{a}{b} = 1$. *Thus,* $f(x) = \lambda(x)\mu(x)$, *where* $\lambda(x)$ *and* $\mu(x)$ *have integer coefficients.*

Definition .70 *A polynomial is said to be an integer monic if all its coefficients are integers and its content is 1.*

Theorem .47 (Eisenstein Criterion) *Let* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *be a polynomial with integer coefficients. Suppose that for some prime* p, $p \mid a_0, a_1, \cdots, a_{n-1}$ *but* $p \nmid a_n$ *and* $p^2 \nmid a_0$. *Then* $f(x)$ *is irreducible over the rationals.*

Proof: *Without loss of generality, let's assume that* $f(x)$ *is primitive since taking out the greatest common divisor of its coefficients does not affect the hypothesis.*
If $f(x)$ *factors as a product of two rational polynomials (due to Gauss's Lemma), then* $f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots c_sx^s)$ *where* b_i, c_i *are integers and* r, s *are both greater than 0.*
Considering $a_0 = b_0c_0$, *we observe that* $p \mid a_0 \Rightarrow p \mid b_0c_0 \Rightarrow p \mid b_0$ *or* $p \mid c_0$.
The condition $p^2 \nmid a_0$ *ensures that* p *cannot divide both. Let's consider the case where* $p \mid b_0$ *and* $p \nmid c_0$.
If all coefficients $b_0, b_1, \cdots, b_r$ *were divisible by* p, *then all coefficients of* $f(x)$ *would be divisible by* p, *which contradicts our hypothesis.*
Therefore, let b_k *be the first coefficient that is not divisible by* p $(0 < k \le r \le n)$. *Now, considering* $a_k = b_kc_0 + b_{k-1}c_1 + \cdots + b_0c_k$, *we see that* $p \mid a_k, p \mid b_0, p \mid b_1, \cdots, p \mid b_{k-1} \Rightarrow p \mid b_kc_0$. *Since* $p \nmid c_0$, *we deduce that* $p \mid b_k$, *which leads to a contradiction.*
This shows that f *is irreducible in* $\mathbb{Z}[x]$. *Let* $f = df_1$, *where* $d \in \mathbb{Z}$ *and* f_1 *is primitive in* $\mathbb{Z}[x]$. *Now, if* f_1 *is irreducible over* $\mathbb{Z}[x]$, *it is also irreducible over* $\mathbb{Q}[x]$, *where* $\mathbb{Q}$ *is the field of quotients of* $\mathbb{Z}$. *Since* $f_1 = \frac{1}{d}f$, *we conclude that* f *is irreducible over* $\mathbb{Q}[x]$.

Theorem .48 *Let* R *be a unique factorization domain, and* K *be its field of quotients. An irreducible primitive polynomial in* $R[x]$ *is also an irreducible polynomial in* $K[x]$.

Proof: *Assume* $f = gk$ *in* $K[x]$, *where* $deg(g) > 0$ *and* $deg(k) > 0$. *Since* K *is the field of quotients of* R, *there exist* d *and* d' *in* R *such that* (dg) *and* $(d'h) \in R[x]$, *i.e.,* $dd'f = (dg)(dh)$. *Also,* $dg = \alpha g_1$, *and* $dh = \beta h_1$ *where* g_1, h_1 *are primitive in* $R[x]$, *and* $\alpha, \beta \in R$. *Thus,* $dd'f = (\alpha\beta)(g_1h_1) \Rightarrow udd' = \alpha\beta$, *where* f_1, g_1, h_1 *are primitive in* $R[x]$, *and* u *is a unit. This implies* $f = \mu(g_1h_1)$. *However, since* f *is irreducible over* $R[x]$, *we conclude that* $deg(\mu g_1) = deg(g_1) = 0$ *or* $deg(h_1) = 0$, *leading to a contradiction.*

*************CHAPTER END**********