1. An example of a rng with no maximal ideal

Zorn’s lemma shows that a ring has a maximal ideal. But it is possible for a rng (ring without unity) to have no maximal ideal.

**Definition 1.1.** An abelian group $G$ is called divisible if for all $x \in G$, $n \in \mathbb{N}$, there is $y \in G$ such that $x = ny = y + y + \cdots + y$ (or $x = y^n$ if we use multiplicative notation).

**Example 1.2.** $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ and any field of characteristic 0 (considered as an additive group) are divisible. $\mathbb{Q}/\mathbb{Z}$, $\mathbb{Z}_{p\infty}$ and any vector space over a field of characteristic 0 are also divisible. But $(\mathbb{Z}/p\mathbb{Z}, +)$, $(\mathbb{Q}^\times, \cdot)$ and $(\mathbb{R}^\times, \cdot)$ are not divisible.

**Proposition 1.3.** Let $G$ be a divisible abelian group. Then $G$ does not have a maximal subgroup. (i.e., for any proper subgroup $H$ of $G$, there is a proper subgroup $H'$ of $G$ properly containing $H$.)

**Proof.** Suppose $H \subseteq G$ is a maximal subgroup. By Correspondence Principle, $G/H$ is simple and abelian, thus isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$. Choose $g \in G \setminus H$, then there is $g' \in G$ such that $pg' = g$. But $pg' \in H$ since $(G : H) = p$. Contradiction! □

**Proposition 1.4.** Let $G$ be a divisible abelian group. Define $x \cdot y = 0$ for all $x, y \in G$. Then $G$ is a rng without a maximal ideal.

Updated: Mar 14, 2014
Theorem 2.4. If

Theorem 2.3. If

For any $x, y \in R$, we have $0 = (x + y)^2 - (x + y) = xy + yx = xy - yx$

since $x^2 = x, y^2 = y$ and $2yx = 0$.

From now on, we let $R$ be a rng ($R$ doesn’t have to have $1_R$). Also let $Z(R)$ be the center of $R$. Note that $Z(R) = \{a \in R \mid ar = ra\text{ for all } r \in R\}$ is a subring of $R$.

Lemma 2.2. Suppose $x^n = x$ for all $x \in R$ for some $n \geq 2$. Then,

1. if $ab = 0$ for $a, b \in R$, then $ba = 0$.
2. if $a^2 = ka$ for $a \in R, k \in \mathbb{Z}$, then $ka \in Z(R)$.
3. $a^{n-1} \in Z(R)$ for all $a \in R$.

Proof. (1) $ba = (ba)^n = b(ab)^{n-1}a = 0$.

(2) For any $x \in R, 0 = (ka)x - a^2x = a(kx - ax)$ and $0 = x(ka) - xa^2 = (kx - xa)a$. By (1), we have

$$x(ka) - axa = (kx - ax)a = 0 = a(kx - xa) = (ka)x - axa$$

thus $x(ka) = (ka)x$.

(3) $(a^{n-1})^2 = a^{2n-2} = a^n \cdot a^{n-2} = a \cdot a^{n-2} = a^{n-1}$. By (2), $a^{n-1} \in Z(R)$.

Theorem 2.3. If $x^3 = x$ for all $x \in R$, then $R$ is commutative.

Proof. Note that $a^2 \in Z(R)$ for all $a \in R$ by 2.2. Thus we have

$$xy = (xy)^2 = x(yx)^2y = (yx)^2xy = yxy^2y = yx^3y^2 = y^3x^3 = xy$$

for any $x, y \in R$.

Theorem 2.4. If $x^4 = x$ for all $x \in R$, then $R$ is commutative.

Proof. For any $a \in R$, we have $-a = (-a)^4 = a^4 = a$. Since $(a^2 + a)^2 = a^4 + 2a^3 + a^2 = a^2 + a$, $a^2 + a \in Z(R)$ for all $a \in R$ by 2.2. Also we have

$$ab + ba = ((a + b)^2 + (a + b)) - (a^2 + a) - (b^2 + b) \in Z(R)$$

for any $a, b \in R$. For $x, y \in R$, we have

$$xy = x^4 y = x^4 y + x^2 y^2 - x^2 y^2 = x^2(y^3 + y^2) - x^4 y^2 = (x^2 y + yx^2)x^2 - x^2 y^2 = yx^4 = yx$$

since $x^2 y + yx^2 \in Z(R)$.

Theorem 2.5. If $x^5 = x$ for all $x \in R$, then $R$ is commutative.
Proof. Note that $(a^4 + a^2)^2 = a^8 + 2a^6 + a^4 = 2(a^4 + a^2)$, thus $2(a^4 + a^2) \in Z(R)$ for all $a \in R$ by 2.2(2). Also by 2.2(3), $2a^2 = 2(a^4 + a^2) - 2a^4 \in Z(R)$ for all $a \in R$. Furthermore,
\[ 4a^3 = 2(a^2 + a)^2 - 2a^4 - 2a^2 \in Z(R) \]
\[ 2a^3 + a^2 + 5a = (a^2 + a)^5 - (a^2 + a) - 10a^4 - 2(4a^3) - 2(2a^2) \in Z(R) \]
for all $a \in R$. Also,
\[ 2(a^2 + a)^3 + (a^2 + a)^2 + 5(a^2 + a) = 7a^4 + 4a^3 + 8a^2 + 11a \in Z(R) \]
for all $a \in R$. Finally, we have
\[ a = (7a^4 + 4a^3 + 8a^2 + 11a) - 7a^4 - 3(2a^2) - 2(2a^3 + a^2 + 5a) \in Z(R) \]
for all $a \in R$. Thus, $R$ is commutative.

\[ \square \]

Theorem 2.6. If $x^6 = x$ for all $x \in R$, then $R$ is commutative.

Proof. For any $a \in R$, we have $-a = (-a)^6 = a^6 = a$. Also,
\[ 0 = (a^2 + a)^6 - (a^2 + a) = 6a^{11} + 15a^{10} + 20a^9 + 15a^8 + 6a^7 = a^5 + a^3 \]
for all $a \in R$. Thus, $a = a^6 = a \cdot a^5 = a \cdot a^3 = a^4$ for all $a \in R$. By 2.4, $R$ is commutative.

\[ \square \]

Question 2.7. What if $x^7 = x$ for all $x \in R$?

In general, the following theorem holds.

Theorem 2.8 (Jacobson). Let $R$ be a rng. Assume that for each $x \in R$, there is $n(x) \in \mathbb{Z}_{\geq 2}$ such that $x^{n(x)} = x$ ($n(x)$ is not fixed!). Then $R$ is commutative.

Proof. See [1].

\[ \square \]

3. SUMS OF TWO SQUARES

Theorem 3.1. $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. We will show that the norm function $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ is a Euclidean function on $\mathbb{Z}[i]$. Given $x = a + bi, y = c + di \in \mathbb{Z}[i]$, let $\frac{y}{x} = r + si$ for $r, s \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ so that $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Let $q = m + ni$ and $r = y - qx$, then
\[ N(r) = N(x)N\left(\frac{y}{x} - q\right) = N(x)N((r - m) + (s - n)i) \leq \frac{1}{2}N(x) \]

Since every Euclidean domain is a PID, $\mathbb{Z}[i]$ is a PID (and also is a UFD). We will use this to classify sums of two squares in $\mathbb{Z}$.

Theorem 3.2. Let $n \in \mathbb{N}$ and write $n = 2^{e_0}p_1^{f_1} \cdots p_k^{f_k}q_1^{j_1} \cdots q_s^{j_s} \in \mathbb{Z}$ where $p_i \equiv 1(\mod 4)$, $q_j \equiv 3(\mod 4)$ are odd primes. Then, $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $f_j$'s are even.
Proof. **Step 1**: If \( p \equiv 1(\text{mod} \ 4) \) is a prime, then \( p \mid x^2 + 1 \) for some \( x \in \mathbb{Z} \).

\[
-1 \equiv (p - 1)! \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2) \cdot (p-1) \\
\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \left( -\frac{p-1}{2} \right) \cdots (-2) \cdot (-1) \\
\equiv (-1)^{\frac{p-1}{2}} \left( 1 \cdot 2 \cdots \frac{p-1}{2} \right)^2 \\
\equiv \left( 1 \cdot 2 \cdots \frac{p-1}{2} \right)^2 \pmod{p}
\]

**Step 2**: If \( p \equiv 1(\text{mod} \ 4) \) is a prime, then \( p \) is a sum of two squares.

By Step 1, \( p \mid x^2 + 1 = (x+i)(x-i) \) in \( \mathbb{Z}[i] \) for some \( x \in \mathbb{Z} \). Since \( p \nmid x+i, x-i \in \mathbb{Z}[i], p \) is not prime. Since \( \mathbb{Z}[i] \) is a PID, \( p \) is not irreducible. Thus, we can write \( p = \alpha \beta \) for some nonunits \( \alpha, \beta \in \mathbb{Z}[i] \). We have \( p^2 = N(p) = N(\alpha)N(\beta) \). Because \( N(r) = 1 \) if and only if \( r \in \mathbb{Z}[i]^\times \), we have \( N(\alpha) = N(\beta) = p \). If \( \alpha = u + vi \) for \( u, v \in \mathbb{Z} \), then \( p = N(\alpha) = u^2 + v^2 \).

**Step 3**: "if" part of the theorem.

By Step 2, \( p \)'s are sums of two squares, and so is \( 2 = 1^2 + 1^2 \). The equality \((x^2 + y^2)(z^2 + w^2) = (xz + yw)^2 + (xw - yz)^2 \) shows that the product of sums of two squares is also a sum of two squares. We can write \( 2^{\alpha_1}p_1^{f_1} \cdots p_s^{f_s} = \alpha^2 + \beta^2 \) for some \( \alpha, \beta \in \mathbb{N} \). If \( f_j \)'s are even, then

\[
n = (\alpha q_1^{f_1/2} \cdots q_s^{f_s/2})^2 + (\beta q_1^{f_1/2} \cdots q_s^{f_s/2})^2
\]

**Step 4**: "only if" part of the theorem.

Suppose \( n = x^2 + y^2 \) and \( d = (x, y), x = dx_0, y = dy_0, \) then \( n = d^2(x_0^2 + y_0^2) \) and \( (x_0, y_0) = 1 \). If \( p \mid x_0^2 + y_0^2 \) for some odd prime \( p \), then \( p \nmid x_0, y_0 \). (otherwise, \( p \) will divide both of them.) In \( \mathbb{Z}/p\mathbb{Z} \), we have \( \overline{x_0}^2 = -\overline{y_0}^2 \).

\[
\overline{1} = \left( \frac{x_0}{y_0} \right)^{p-1} = \left( \frac{x_0}{y_0} \right)^2 \cdot (-1)^{\frac{p-1}{2}} = (-\overline{1})^{\frac{p-1}{2}}
\]

in \( \mathbb{Z}/p\mathbb{Z} \) shows that \( p \equiv 1 \pmod{4} \). This shows that \( q_j \)'s cannot divide \( x_0^2 + y_0^2 \), thus should divide \( d^2 \). So we have \( 2 \mid f_j \) for all \( j \).

The followings are generalizations of this type of classification.

**Theorem 3.3.** \( n \in \mathbb{N} \) is a sum of three squares if and only if \( n \neq 4^m(8k + 7) \) for \( m, k \in \mathbb{Z}_{\geq 0} \).

**Theorem 3.4.** Every positive integer is a sum of four (thus, or more) squares.

**Theorem 3.5.** For each \( n \in \mathbb{N} \), there is an integer \( g(n) \in \mathbb{N} \) such that every positive integer \( n \) is a sum of \( g(n) \) \( n \)th powers.

4. An example of a PID which is not a Euclidean domain

Let \( \theta = \frac{-1 + \sqrt{-19}}{2} \) and \( R = \mathbb{Z}[\theta] = \{ a + b\theta \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{C} \). We will show that \( R \) is a PID, but is not a Euclidean domain.

**Lemma 4.1.** (1) \( R^\times = \{ \pm 1 \} \)

(2) \( 2, 3 \in R \) are irreducible.
Proof. (1) Consider the norm function \( N : R \to \mathbb{R} \) defined by \( N(r) = r\bar{r} \) where \( \bar{r} \) is the complex conjugate of \( r \). For \( a + b\theta \in R \), we have
\[
N(a + b\theta) = N \left( \left( a - \frac{b}{2} \right) - \frac{b\sqrt{-19}}{2} \right) = \frac{(2a - b)^2 + 19b^2}{4} = a^2 - ab + 5b^2 \in \mathbb{Z}_{\geq 0}
\]
We can see that \( N \) is a multiplicative homomorphism, thus for \( x, y \in R \), \( N(x) | N(y) \) in \( \mathbb{Z} \) if \( x | y \) in \( R \). If \( N(\alpha) = 1 \) for some \( \alpha \in R \), then \( \alpha \in R^x \) since \( \alpha\bar{\alpha} = 1 \) and \( \bar{\alpha} \in R \). Conversely, if \( \alpha \in R^x \), then there \( N(\alpha) | N(1) = 1 \) in \( \mathbb{Z} \), thus we have \( N(\alpha) = \pm 1 \).
Write \( \alpha = a + b\theta \), then \( \alpha \in R^x \) if and only if \( N(\alpha) = 1 \) if and only if \( (2a - b)^2 + 19b^2 = 4 \) if and only if \( a = \pm 1, b = 0 \) if and only if \( \alpha = \pm 1 \).

(2) Suppose \( 2 = \alpha\beta \) for \( \alpha, \beta \in R \). We have \( 4 = N(2) = N(\alpha)N(\beta) \). Note that no element in \( R \) has norm 2 because \( 2 = (2a - b)^2 + 19b^2 = 8 \) has no integer solution. Thus, \( N(\alpha) = 1 \) or \( N(\beta) = 1 \), i.e., \( \alpha \in R^x \) or \( \beta \in R^x \). Therefore, 2 is irreducible. Similarly, so is 3.

**Theorem 4.2.** \( R \) is not a Euclidean domain.

**Proof.** Suppose \( R \) has a Euclidean function \( \delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0} \) satisfying the division algorithm. Choose \( m \in R \setminus (R^x \cup \{0\}) \) with minimal \( \delta(m) \).
There are \( q, r \in R \) such that \( 2 = mq + r \) with \( r = 0 \) or \( \delta(r) < \delta(m) \). By the choice of \( m \), we have either \( r = 0 \) or \( r \in R^x = \{\pm 1\} \). If \( r = 0 \), then we have \( 2 = mq \). Since 2 is irreducible and \( m \) is not a unit, we have \( q = \pm 1 \), \( m = \mp 2 \).
If \( r = -1 \), then we have \( 3 = mq \). By the similar argument, we have \( q = \pm 1 \) and \( m = \mp 3 \).

Now we apply the division algorithm for \( \theta \). There are \( q_0, r_0 \in R \) such that \( \theta = mq_0 + r_0 \), and similarly, \( r = 0, -1, 1 \). We have \( mq = \theta + r \). The norm of the left-hand side is \( N(mq) = N(m)N(q) \), thus divisible either by \( 4 = N(\pm 2) \) or by \( 9 = N(\pm 3) \). On the other hand, we have \( N(\theta) = N(\theta + 1) = 5 \) and \( N(\theta - 1) = 7 \) on the right-hand side. Contradiction!

**Theorem 4.3.** \( R \) is a PID.

**Proof.** Let \( \mathfrak{a} \) be an ideal of \( R \) and choose \( 0 \neq a \in \mathfrak{a} \) with minimal \( N(a) \). Choose \( b \in \mathfrak{a} \). We will show that \( b \in (a) \). Since \( \text{Im} f = -\sqrt[4]{19} \), there is an integer \( m \in \mathbb{Z} \) such that \( |\text{Im}(\frac{b}{a} + m\theta)| \leq \frac{\sqrt[4]{19}}{4} \).

**Case 1:** \( |\text{Im}(\frac{b}{a} + m\theta)| < \frac{\sqrt[4]{3}}{2} \)
There is an integer \( n \in \mathbb{Z} \) such that \( |\text{Re}(\frac{b}{a} + m\theta + n)| \leq \frac{1}{2} \). Thus \( N(\frac{b}{a} + m\theta + n) < 1 \), and \( N(b + a(m\theta + n)) < N(a) \). Since \( b + a(m\theta + n) \in \mathfrak{a} \) and \( N(a) \) is minimal, we have \( b = -a(m\theta + n) \in (a) \).

**Case 2:** \( \sqrt{3} \leq |\text{Im}(\frac{b}{a} + m\theta)| \leq \sqrt[4]{19} \)
We have
\[
-\frac{\sqrt{3}}{2} < \sqrt{3} - 3\sqrt{3} < \sqrt{3} - \frac{\sqrt{19}}{2} \leq \text{Im} \left( 2 \left( \frac{b}{a} + m\theta \right) + \theta \right) \leq 0
\]
There is \( n \in \mathbb{Z} \) such that \( |\text{Re}(\frac{b}{a} + 2m\theta + \theta + n)| \leq \frac{1}{2} \). By the same argument with Case 1, we have \( N(2b + a(2m\theta + \theta + n)) < N(a) \) and \( -b - am\theta = \frac{a(\theta + n)}{2} \in \mathfrak{a} \). If \( n \) is even, then \( \frac{a\theta}{2} \in \mathfrak{a} \) and \( \frac{n}{2} = \frac{(a\theta + 1)}{2} \in \mathfrak{a} \), which is a contradiction since \( 0 < N\left(\frac{\theta}{2}\right) < N(a) \). If \( n \) is odd, then \( \frac{a(\theta + 1)}{2} \in \mathfrak{a} \) and \( \frac{n}{2} = \frac{(a\theta + 1)}{2} \in \mathfrak{a} \), which is also a contradiction.

**Case 3:** \( -\frac{\sqrt[4]{19}}{4} \leq |\text{Im}(\frac{b}{a} + m\theta)| \leq -\frac{\sqrt{3}}{2} \)
Apply Case 2 for \( -(\frac{b}{a} + m\theta) \).
5. Polynomial Functions

Let \( R \) be a ring and \( \text{Func}(R, R) = \{ f : R \to R \mid f \text{ is a function} \} \) (we don’t assume any property of \( f \)) be the ring of functions from \( R \) to \( R \). The ring structure of \( \text{Func}(R, R) \) is given pointwise: \((f + g)(a) = f(a) + g(a), (fg)(a) = f(a)g(a)\). We consider the map

\[
\Phi = \Phi_R : R[t] \to \text{Func}(R, R)
\]

\( f(t) \mapsto (\Phi(f) : a \mapsto f(a)) \)

**Definition 5.1.** A function \( f \in \text{Func}(R, R) \) is called a polynomial function if \( f \in \text{Im} \Phi \).

**Example 5.2.** \( \Phi \) is not surjective in general. Let \( R = \mathbb{R} \) and consider \( \exp \in \text{Func}(\mathbb{R}, \mathbb{R}) \) where \( \exp(a) = e^a \). For any polynomial \( f(t) \in \mathbb{R}[t] \), we have \( \lim_{t \to \infty} \frac{e^t}{f(t)} = \infty \), thus \( \exp \notin \text{Im} \Phi \).

**Example 5.3.** \( \Phi \) is not injective in general. Let \( R = \mathbb{Z}/p\mathbb{Z} \), then we have \( x^p = x \) for all \( x \in \mathbb{Z}/p\mathbb{Z} \). Therefore, \( \Phi(x^p) = \Phi(x) \).

**Example 5.4.** \( \Phi \) is in general not a ring homomorphism. Suppose that \( R \) is not commutative, and \( ab \neq ba \) for \( a, b \in R \). Consider \( f(t) = t, g(t) = a \in R[t] \). Then, we have \( (\Phi(f)\Phi(g))(b) = (\Phi(f)(b))(\Phi(g)(b)) = ba \neq ab = \Phi(fg)(b) \).

If \( R \) is an infinite domain or a finite field, then we can say something more about the function \( \Phi \).

**Theorem 5.5.** If \( R \) is an infinite domain, then \( \Phi \) is injective.

Proof. Suppose \( f(t), g(t) \in \mathbb{R}[t] \) and \( \Phi(f) = \Phi(g) \). This means we have \((f - g)(a) = 0\) for all \( a \in R \). If \( f(t) - g(t) \neq 0 \), then \( f - g \) can have at most \( \operatorname{deg}(f - g) \) distinct roots. Since \( R \) is infinite, we have \( f(t) = g(t) \). \( \square \)

**Theorem 5.6.** Let \( R = \mathbb{F}_q \) be a (the) finite field of order \( q \), then we have \( \ker \Phi = (t^q - t) \) and \( \Phi \) is surjective. Therefore, we have \( \mathbb{F}_q[t]/(t^q - t) \cong \text{Func}(\mathbb{F}_q, \mathbb{F}_q) \).

Proof. (In 110C, we will see that \( q \) must be a power of prime, and there are only one finite field of order \( q \) up to isomorphism. But we won’t need these facts for the proof of this theorem.)

Note that \( |\mathbb{F}_q^\times| \) is a multiplicative group of order \( q - 1 \). Thus for any \( a \in \mathbb{F}_q^\times \), we have \( a^{q-1} = 1 \). This means \( t^q - t \in \mathbb{F}_q[t] \) has all the elements of \( \mathbb{F}_q \) as its roots, so \((t^q - t) \subseteq \ker \Phi \). Suppose \( g(t) \in \ker \Phi \). By euclidean algorithm, there are \( q(t), r(t) \in \mathbb{F}_q[t] \) such that \( g(t) = (t^q - t)q(t) + r(t) \) and \( r = 0 \) or \( \deg r < \deg(t^q - t) = q \). Since \( g(a) = 0 = a^q - a \) for all \( a \in \mathbb{F}_q \), we get \( r(a) = 0 \) for all \( a \in \mathbb{F}_q \) by evaluating \( t = a \) to the above equation. If \( r \neq 0 \), then \( r \) can only have \( \deg r < q \) distinct roots in \( \mathbb{F}_q \). Thus we have \( r = 0 \) and \( g \in (t^q - t) \).

By the first isomorphism theorem, we have

\[
\mathbb{F}_q[t]/(t^q - t) \cong \text{Im} \Phi \subseteq \text{Func}(\mathbb{F}_q, \mathbb{F}_q)
\]

Now we can compare two sides by counting the number of elements. Note that for any \( f(t) \in \mathbb{F}_q[t] \), we can find \( r(t) \in \mathbb{F}_q[t] \) such that \( \bar{f}(t) = \bar{r}(t) \) in \( \mathbb{F}_q[t]/(t^q - t) \) and \( \deg r < q \) by euclidean algorithm. Also any \( r_1(t) \neq r_2(t) \in \mathbb{F}_q[t] \) with \( \deg r_1 < q \) and \( \deg r_2 < q \), we have \( r_1(t) \neq r_2(t) \) in \( \mathbb{F}_q[t]/(t^q - t) \) because the difference \( r_1 - r_2 \) has degree less than \( q \), thus cannot be in \( (t^q - t) \).

\[
|\mathbb{F}_q[t]/(t^q - t)| = |\text{Im} \Phi| \leq |\text{Func}(\mathbb{F}_q, \mathbb{F}_q)| = q^q = |\mathbb{F}_q[t]/(t^q - t)|
\]

On the other hand, we have

\[
|\mathbb{F}_q[t]/(t^q - t)| = |\text{Im} \Phi| \leq |\text{Func}(\mathbb{F}_q, \mathbb{F}_q)| = q^q = |\mathbb{F}_q[t]/(t^q - t)|
\]
There exists a polynomial in

\[ \text{Example } 5.8 \]

interpolation. Now we define defining

\[ \text{Example } 5.9 \]

points.

Similarly, we can get

\[ \text{Corollary } 5.7. \]

This shows the surjectivity of \( \Phi \). □

Let \( F \) be a field (not necessarily finite) and consider the pairs \((x_0,y_0),(x_1,y_1),\ldots,(x_k,y_k)\) in \( F \times F \) where \( x_i \neq x_j \) if \( i \neq j \). Then we can find a polynomial \( L(t) \in F[t] \) such that \( L(x_i) = y_i \) for all \( i = 0, \ldots, k \) with \( \deg L \leq k \). We first define

\[
l_i(t) = \prod_{\substack{j \neq i \\text{or } 0 \leq j \leq k}} \frac{t - x_j}{x_i - x_j} \in F[t]
\]

Note that the denominator is not zero by assumption. Then we get

\[
l_i(x_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}
\]

Now we define \( L(t) = \sum_{i=0}^{k} y_i l_i(t) \), then \( L(x_i) = y_i \) is satisfied for all \( i \). This is called Lagrange interpolation.

\[ \text{Example } 5.8. \]

Consider \( k + 1 \) points on the \( xy \)-plane whose \( x \)-coordinates are distinct. Then there exists a polynomial in \( \mathbb{R}[t] \) with degree at most \( k \) whose graph passes through those \( k + 1 \) points.

\[ \text{Example } 5.9. \]

Consider the function \( f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \) defined by \( f(0) = 3, f(1) = 0, f(2) = 1, f(3) = 1, f(4) = 0 \). We apply the method above to find a polynomial in \( L_f(t) \in \mathbb{Z}/5\mathbb{Z}[t] \) defining \( f \). Firstly, we have

\[
l_0(t) = \frac{(t - 1)(t - 2)(t - 3)(t - 4)}{(0 - 1)(0 - 2)(0 - 3)(0 - 4)} = -t^4 + 1
\]

Similarly, we can get \( l_2(t) = -(t^3 - t)(t + 2) \) and \( l_3(t) = -(t^3 - t)(t - 2) \). Therefore,

\[
L_f(t) = 3l_0(t) + l_2(t) + l_3(t) = 2t^2 + 3
\]

We can easily check that we have indeed \( L_f(a) = f(a) \) for all \( a \in \mathbb{Z}/5\mathbb{Z} \).

A more general thing also holds, and the proof is similar (count the number of elements!).

\[ \text{Theorem } 5.10. \]

Define \( \Phi_n : \mathbb{F}_q[t_1, \ldots, t_n] \to \text{Func}(\mathbb{F}_q^n, \mathbb{F}_q) \) similarly. Then \( \Phi_n \) is surjective and \( \ker \Phi_n = (t_1^q - t_1, t_2^q - t_2, \ldots, t_n^q - t_n) \). Thus we have

\[
\mathbb{F}_q[t_1, t_2, \ldots, t_n]/(t_1^q - t_1, t_2^q - t_2, \ldots, t_n^q - t_n) \cong \text{Func}(\mathbb{F}_q^n, \mathbb{F}_q)
\]

6. Classes of rings

(1) Field \( \subset (2) \) Euclidean domain \( \subset (3) \) PID \( \subset (4a) \) Noetherian domain, (4b) UFD

\( \subset (5) \) Integral domain \( \subset (6) \) Commutative ring \( \subset (7) \) All rings
(1) \implies (2) \implies (3) \implies (4a) \text{ or } (4b) \implies (5) \implies (6) \implies (7) \text{ Clear}

(2) \not\implies (1) \mathbb{Z}

(3) \not\implies (2) \mathbb{Z}[\frac{-1+\sqrt{19}}{2}] \text{ by the previous section.}

(4a) \not\implies (3), (4b) \not\implies (3) \text{ Since } \mathbb{Z} \text{ is a UFD and a Noetherian domain, } \mathbb{Z}[t] \text{ is also a UFD (2 Ch 30) and a Noetherian domain (Hilbert basis theorem). But } (2, t) \subseteq \mathbb{Z}[t] \text{ is not principal.}

(4a) \not\implies (4b)

(4b) \not\implies (3) \text{ is Noetherian because } \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[t]/(t^2 + 5) \text{ and } \mathbb{Z}[t] \text{ is Noetherian, but is not a UFD because } 1 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \text{ is irreducible, but not prime. (1 + \sqrt{-5} | 6 = 2 \cdot 3 \text{ but } 1 + \sqrt{-5} \not| 2, 3)}

(4b) \not\implies (4a)

(4b) \not\implies (3) \text{ is a UFD because any polynomial has only finitely many variables and } \mathbb{Z}[t_1, t_2, \ldots, t_n] \text{ is a UFD for all } n \text{ by induction. But it is not Noetherian because we have a strictly increasing sequence of ideals } (t_1) \subsetneq (t_1, t_2) \subsetneq \ldots.

(5) \not\implies (4a), (5) \not\implies (4b) \text{ The examples above work.}

(6) \not\implies (5) \mathbb{Z}/4\mathbb{Z}

(7) \not\implies (6) M_2(\mathbb{R})

7. EXAMPLES OF DIAGRAM CHASING

Let \( R \) be a ring. All arrows in this section are \( R \)-module homomorphisms.

**Theorem 7.1** (Five lemma). Suppose we have the following commutative diagram of \( R \)-modules with exact rows.

\[
\begin{array}{cccccc}
A & \overset{f}{\longrightarrow} & B & \overset{g}{\longrightarrow} & C & \overset{h}{\longrightarrow} & D & \overset{i}{\longrightarrow} & E \\
\downarrow{\alpha_1} & & \downarrow{\alpha_2} & & \downarrow{\alpha_3} & & \downarrow{\alpha_4} & & \downarrow{\alpha_5} \\
A' & \overset{f'}{\longrightarrow} & B' & \overset{g'}{\longrightarrow} & C' & \overset{h'}{\longrightarrow} & D' & \overset{i'}{\longrightarrow} & E'
\end{array}
\]

Then the following holds.

1. If \( \alpha_2, \alpha_4 \) are surjective and \( \alpha_5 \) is injective, then \( \alpha_3 \) is surjective.
2. If \( \alpha_2, \alpha_4 \) are injective and \( \alpha_1 \) is surjective, then \( \alpha_3 \) is injective.
3. If \( \alpha_2, \alpha_4 \) are bijective, \( \alpha_5 \) is injective and \( \alpha_1 \) is surjective, then \( \alpha_3 \) is bijective.

**Proof.** Diagram chasing! \( \square \)

**Theorem 7.2** (Nine lemma). Suppose we have the following commutative diagram of \( R \)-modules.

\[
\begin{array}{cccccc}
0 & 0 & 0 & 0 & 0 & 0 \\
\downarrow & & & & \downarrow & \\
0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\
\downarrow & & & & \downarrow & \\
0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \\
\downarrow & & & & \downarrow & \\
0 & \longrightarrow & A_3 & \longrightarrow & B_3 & \longrightarrow & C_3 & \longrightarrow & 0 \\
\downarrow & & & & \downarrow & \\
0 & 0 & 0 & 0 & 0 & 0
\end{array}
\]
If all columns and two bottom rows are exact, then so is the top row. If all columns and two top rows are exact, then so is the bottom row.

Proof. Another diagram chasing! \( \square \)

**Theorem 7.3** (Snake lemma). Suppose we have the following commutative diagram of \( R \)-modules with exact rows.

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
\downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C'
\end{array}
\]

Then, we have the following exact sequence of \( R \)-modules.

\[ 0 \rightarrow \ker f \hookrightarrow \ker \alpha \xrightarrow{\tilde{f}} \ker \beta \xrightarrow{\tilde{g}} \ker \gamma \xrightarrow{\delta} \coker \alpha \xrightarrow{\tilde{f}'_\beta} \coker \beta \xrightarrow{\gamma} \coker \gamma \xrightarrow{id_C} \coker g' \rightarrow 0 \]

The maps are defined as follows. \( \tilde{f} = f|_{\ker \alpha}, \tilde{g} = g|_{\ker \beta} \) and \( \tilde{f}', \tilde{g}', \gamma = id_C \) are the quotient maps of \( f', g', id_C \). Given \( c \in \ker \gamma \), choose \( b \in B \) such that \( g(b) = c \). By commutativity of the diagram, we have \( g'\beta(b) = \gamma g(b) = \gamma(c) = 0 \). Thus, \( \beta(b) \in \ker g' = \text{Im} f' \). Define \( \delta(c) = a' \in A'/\text{im} \alpha \) so that \( \beta(b) = f'(a') \).

Proof. Well-definedness of the maps above and the exactness of the sequence can be checked by diagram chasing!

For example, let’s check the exactness at \( \ker \gamma \). Firstly, let \( c = \tilde{g}(b) \) for \( b \in \ker \beta \). By definition of the map \( \delta \), \( \delta(c) = a' \) where \( f'(a') = \beta(b) = 0 \). We have \( a' = 0 \) since \( f' \) is injective, thus \( c \in \ker \delta \).

On the other hand, suppose \( d(c) = 0 \). By definition of \( \delta \), there are \( a' \in \text{im} \alpha \) and \( b \in B \) such that \( g(b) = c \) and \( f'(a') = \beta(b) \). Choose \( a \in A \) satisfying \( \alpha(a) = a' \). Since \( \beta(b) = f'\alpha(a) = \beta f(a) \), we have \( b - f(a) \in \ker \beta \) and \( g(b - f(a)) = g(b) - gf(a) = g(b) \in C \). Thus, \( c = g(b) = \tilde{g}(b) \in \text{im} \tilde{g} \).

Other parts of the proof are similar. \( \square \)

**Theorem 7.4** (Kernel-cokernel lemma). Suppose that we have \( R \)-module homomorphisms \( A \xrightarrow{f} B \xrightarrow{g} C \) (not necessarily exact). Then we have the following exact sequence.

\[ 0 \rightarrow \ker f \rightarrow \ker g \circ f \rightarrow \ker g \rightarrow \coker f \rightarrow \coker g \circ f \rightarrow \coker g \rightarrow 0 \]

Proof. Apply the snake lemma to the following commutative diagram.

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B & \longrightarrow & \coker f & \longrightarrow & 0 \\
\downarrow{gf} & & \downarrow{g} & & \downarrow & & \\
0 & \longrightarrow & C & \xrightarrow{1_C} & C & \longrightarrow & 0
\end{array}
\]

\( \square \)

8. ACC and DCC

**Theorem 8.1.** Let \( M \) be a nonzero \( R \)-module for a ring \( R \). Then, \( M \) has a composition series (a chain of submodules with simple factors) if and only if \( M \) satisfies both the ascending (Noetherian) and descending (Artinian) chain condition.
Proof. Suppose $M$ has a composition series of length $n$. If either chain condition fails to hold, then one can find a chain of submodules with length $n + 1$. The two series have an equivalent refinement which has length at least $n + 1$, but the composition series does not have a proper refinement. Contradiction!

Conversely, suppose that $M$ satisfies both ACC and DCC. Since $M$ is Noetherian, the set of proper submodules of $M$ has a maximal element, say $M_1$. Also the set of proper submodules of $M_1$ has a maximal element $M_2$. In this way, we can construct a strictly decreasing chain of submodules of $M$

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$$

with simple factors. Since $M$ also satisfies DCC, this chain has to stabilize, which gives a finite composition series of $M$. □

9. $\bigoplus_{i=0}^{\infty} \mathbb{Z}$ and $\prod_{i=0}^{\infty} \mathbb{Z}$

Definition 9.1. We define the following $\mathbb{Z}$-modules

$$\prod_{i=0}^{\infty} \mathbb{Z} = \{(a_0, a_1, a_2, \cdots) \mid a_i \in \mathbb{Z}\}$$

$$\bigoplus_{i=0}^{\infty} \mathbb{Z} = \{(a_0, a_1, a_2, \cdots) \mid a_i \in \mathbb{Z}, a_i = 0 \text{ for all but finitely many } i\} \subseteq \prod_{i=0}^{\infty} \mathbb{Z}$$

Note that we have $\bigoplus_{i=0}^{\infty} \mathbb{Z} \cong \mathbb{Z}[t]$, and $\prod_{i=0}^{\infty} \mathbb{Z} \cong \mathbb{Z}[[t]]$ by $(a_i) \mapsto \sum a_i t^i$ as $\mathbb{Z}$-modules (not as rings!).

Remark 9.2. $\mathbb{Z}$ is $\mathbb{Z}$-free with a basis $\{1\}$. Thus, $\bigoplus_{i=0}^{\infty} \mathbb{Z}$ is $\mathbb{Z}$-free with the standard basis $\{e_1\}_{i=0}^{\infty}$ where $e_1 = (0, 0, \cdots, 0, 1, 0, 0, \cdots)$. But $\{e_1\}$ does not span $\prod_{i=0}^{\infty} \mathbb{Z}$ because $(1, 1, 1, \cdots) \notin \langle\{e_1\}\rangle$.

Lemma 9.3. Let $f : \prod_{i=0}^{\infty} \mathbb{Z} \rightarrow \mathbb{Z}$ be a $\mathbb{Z}$-module homomorphism. If $\bigoplus_{i=0}^{\infty} \mathbb{Z} \subseteq \ker f$, then $f = 0$.

Proof. Let $x = (x_i) \in \prod \mathbb{Z}$. Since $\gcd(2^i, 3^i) = 1$ for all $i$, there are $a_i, b_i \in \mathbb{Z}$ such that $a_i 2^i + b_i 3^i = x_i$ for all $i$.

$$f((a_i 2^i)_{i=0}^{\infty}) = f\left(\sum_{i=0}^{k-1} a_i 2^i e_i + \sum_{i \geq k} a_i 2^i e_i\right)$$

$$= \sum_{i=0}^{k-1} a_i 2^i f(e_i) + 2^k f\left(\sum_{i \geq k} a_i 2^{-k} e_i\right) = 2^k f\left(\sum_{i \geq k} a_i 2^{-k} e_i\right)$$

since $e_i \in \ker f$ for all $i$. So $2^k | f((a_i 2^i)_i) \in \mathbb{Z}$ for all $k$, which means $f((a_i 2^i)_i) = 0$. Similarly we have $f((b_i 3^i)_i) = 0$ and $f(x) = f((a_i 2^i)_i) + f((b_i 3^i)_i) = 0$. □
Remark 9.4. We cannot prove that \( f(\sum x_i) = \sum f(x_i) \) for infinite sums! Note that we have this for finite sums by repeatedly using the fact that \( f \) is an additive homomorphism.

Theorem 9.5. \( \prod_{i=0}^{\infty} Z \) is not a free \( Z \)-module.

Proof. Suppose that \( \prod Z \) is free with a basis \( B \). Note that \( \prod Z \) is uncountable (\( \prod Z \) contains \( \prod \{\pm 1\} \), which has cardinality \( \aleph_1 \) ), thus \( B \) is also uncountable. Since each element in \( \bigoplus Z \) can be written as a finite \( Z \)-linear combination of elements in \( B \), and \( \bigoplus Z \) is countable, we have a countable subset \( B_0 \subseteq B \) such that \( \bigoplus Z \subseteq \langle B_0 \rangle \). Choose \( b \in B \setminus B_0 \) and consider the projection \( \pi_b : \prod Z \to Z \) which maps an element of \( \prod Z \) to its coefficient of \( b \). Then \( \pi_b \) is a well-defined \( Z \)-module homomorphism, and \( \bigoplus Z \subseteq \langle B_0 \rangle \subseteq \ker \pi_b \). By 9.3, we should have \( \pi_b = 0 \), but we have \( \pi_b(b) = 1 \). Contradiction! \( \Box \)

Remark 9.6. \( \prod Z \) is an example of a torsion-free \( Z \)-module which is not free. This doesn’t happen in the category of finitely generated modules over \( Z \).

Theorem 9.7. Let \( R = \text{End}_Z \left( \prod_{i=0}^{\infty} Z \right) \), then \( R^m \cong R^n \) as free \( R \)-modules for all \( m, n \in \mathbb{N} \).

(this says that the rank of a free \( R \)-module is not well-defined!)

Proof. Consider the following elements in \( R \).

\[
\begin{align*}
    f_1(a_0, a_1, a_2, \cdots) &= (a_0, a_2, a_4, \cdots) \\
    f_2(a_0, a_1, a_2, \cdots) &= (a_1, a_3, a_5, \cdots) \\
    g_1(a_0, a_1, a_2, \cdots) &= (a_0, 0, a_1, 0, a_2, \cdots) \\
    g_2(a_0, a_1, a_2, \cdots) &= (0, a_0, 0, a_1, 0, a_2, \cdots)
\end{align*}
\]

Note that we have \( f_1 g_1 = f_2 g_2 = 1_R, f_1 g_2 = f_2 g_1 = 0 \) and \( g_1 f_1 + g_2 f_2 = 1_R \). For any \( h \in R \),

\[ h = h \circ 1_R = h(g_1 f_1 + g_2 f_2) = (h g_1) f_1 + (h g_2) f_2 \]

This shows \( \{f_1, f_2\} \) spans \( R \). If we have \( h_1 f_1 + h_2 f_2 = 0 \) for some \( h_1, h_2 \in R \), then \( 0 = 0 \circ g_1 = (h_1 f_1 + h_2 f_2) g_1 = h_1 (f_1 g_1) + h_2 (f_2 g_1) = h_1 \).

Similarly we can show that \( h_2 = 0 \), thus \( \{f_1, f_2\} \) is linearly independent. Therefore we have \( R = R f_1 \bigoplus R f_2 \cong R^2 \) as free \( R \)-modules. By induction, we can show that \( R \cong R^n \), thus \( R^m \cong R^n \) for any \( m, n \in \mathbb{N} \) as free \( R \)-modules. \( \Box \)

Definition 9.8. Let \( M \) be an \( R \)-module. We define the dual \( R \)-module of \( M \) by

\[ M^* = \text{Hom}_R(M, R) = \{ f : M \to R \mid f \text{ is a } R\text{-homomorphism} \} \]

with \( (f + g)(m) = f(m) + g(m), (rf)(m) = rf(m) \) for \( f, g \in M^*, r \in R \).

Theorem 9.9. We have (1) \( \bigoplus_{i=0}^{\infty} Z \cong \prod_{i=0}^{\infty} Z \) and (2) \( \left( \prod_{i=0}^{\infty} Z \right)^* \cong \bigoplus_{i=0}^{\infty} Z \).

Proof. (1) We define

\[ \phi : \text{Hom}_Z \left( \bigoplus Z, Z \right) \to \prod Z \]

\[ f \mapsto (f(e_i))_{i=0}^{\infty} \]

We can see that \( \phi \) is a well-defined \( Z \)-module homomorphism.

If \( \phi(f) = 0 \), then we have \( f(e_i) = 0 \) for all \( i \). Since \( \{e_i\} \) is a basis of \( \bigoplus Z \), we have \( f = 0 \).
Therefore \( \phi \) is injective.

For any \( (n_i)_{i=0}^{\infty} \in \prod \mathbb{Z} \), we define \( g : \bigoplus \mathbb{Z} \rightarrow \mathbb{Z} \) by \( g(\sum a_ie_i) = \sum a_in_i \). Then \( g \) is well-defined (only finitely many \( a_i \)'s are nonzero) and \( g \in \text{Hom}_\mathbb{Z}(\bigoplus \mathbb{Z}, \mathbb{Z}) \). Also we can see that \( \phi(g) = ((g(e_i))_i) = ((n_i)_i) \), thus \( \phi \) is surjective.

(2) We define

\[
\psi : \text{Hom}_\mathbb{Z}(\prod \mathbb{Z}, \mathbb{Z}) \rightarrow \bigoplus \mathbb{Z} \\
\quad f \mapsto (f(e_i))_{i=0}^\infty
\]

We first check well-definedness of \( \psi \). Given \( f \in \text{Hom}_\mathbb{Z}(\prod \mathbb{Z}, \mathbb{Z}) \), we choose integers \( 0 < n_1 < n_2 < \cdots \) satisfying \( \sum_{i=0}^{k-1} 2^{n_i} |f(e_i)| < 2^{n_k-1} \) for each \( k \). Consider \( x = ((2^{n_i})_i) \in \prod \mathbb{Z} \), then

\[
f(x) = f \left( \sum_{i=0}^{k-1} 2^{n_i} e_i + \sum_{i \geq k} 2^{n_i} e_i \right) = \sum_{i=0}^{k-1} 2^{n_i} f(e_i) + 2^{n_k} f \left( \sum_{i \geq k} 2^{n_i-n_k} e_i \right)
\]

call this \( b_k \)

for each \( k \). Because

\[
|f(x)| \geq |2^{n_k} b_k| - \left| \sum_{i=0}^{k-1} 2^{n_i} f(e_i) \right| > 2^{n_k} |b_k| - 2^{n_k-1}
\]

for all \( k \), and \( f(x) \in \mathbb{Z} \), we have \( b_k = 0 \) for sufficiently large \( k \). Since we have \( 2^{n_k} b_k = 2^{n_k} f(e_k) + 2^{n_k+1} b_{k+1}, f(e_k) = 0 \) for sufficiently large \( k \). Thus, \( f \) is well-defined.

We can easily check that \( f \) is a \( \mathbb{Z} \)-module homomorphism from definition.

If \( \psi(f) = 0 \), then we have \( f(e_i) = 0 \) for all \( i \). Thus, \( \bigoplus \mathbb{Z} \subseteq \ker f \), and \( f = 0 \) by 9.3. Therefore \( \psi \) is injective.

For any \( ((m_i)_i) \in \bigoplus \mathbb{Z} \), we define \( g : \prod \mathbb{Z} \rightarrow \mathbb{Z} \) by \( g(\sum a_i e_i) = \sum a_im_i \). Then \( g \) is well-defined (only finitely many \( m_i \)'s are nonzero) and \( g \in \text{Hom}_\mathbb{Z}(\prod \mathbb{Z}, \mathbb{Z}) \). Also we can see that \( \psi(g) = (g(e_i)_i) = ((m_i)_i) \), thus \( \psi \) is surjective. \( \square \)

10. Selected problems from Elman’s note

Problem (21.20.3). Show if \( R \) is a commutative ring, then for any ideal \( \mathfrak{B} \) in \( M_n(R) \), there exists an ideal \( \mathfrak{A} \) in \( R \) satisfying \( \mathfrak{B} = M_n(\mathfrak{A}) \). In particular, if \( R \) is simple, so is \( M_n(R) \). Show that \( M_n(R) \) is never a division ring if \( n > 1 \).

Proof. Let \( E_{ij} \in M_n(R) \) be the matrix with 1 on \( (i,j) \)-th component and 0 on the other components. Then we have

\[
E_{ij}E_{kl} = \begin{cases} 
E_{il} & \text{if } j = k \\
0 & \text{otherwise}
\end{cases}
\]

Let \( \mathfrak{A} \) be the ideal generated by the entries of elements in \( \mathfrak{B} \). Clearly, we have \( \mathfrak{B} \subseteq M_n(\mathfrak{A}) \).

Conversely, let \( A = (a_{ij}) \in M_n(\mathfrak{A}) \). Suppose \( a_{11} = \sum_{s=1}^t r_s b_s \) where \( r_s \in R \) and \( b_s \) is the
If necessary, we can assume that \( m = S \). Proof. Let this shows that \( m \subseteq S \). Therefore, \( a \in R \). Thus \( a \) is simple, then the only ideals of \( M_n(R) \) are \( M_n(\{0\}) = \{0_n\} \) and \( M_n(R) \), thus \( M_n(R) \) is simple. For \( n \geq 2 \), consider \( E_{11} \in M_n(R) \). Suppose \( E_{11}A = I_n \). If \( A = \sum_{i,j} a_{ij}E_{ij} \), then

\[
\sum_{i=1}^{n} E_{ii} = I_n = E_{11}A = \sum_{j=1}^{n} a_{1j}E_{1j}
\]

which is not possible because \( E_{22} \) does not appear in the right-hand side. Therefore, \( E_{11} \) is not invertible, and \( M_n(R) \) is not a division ring. \( \square \)

**Problem** (21.20.13). Let \( a_1, \ldots, a_n \) be ideals in \( R \), at least \( n - 2 \) of which are prime. Let \( S \subseteq R \) be a subring (it does not have to have 1) contained in \( a_1 \cup a_2 \cup \cdots \cup a_n \). Then one of the \( a_j \)'s contains \( S \). In particular, if \( p_1, \ldots, p_n \) are prime ideals in \( R \) and \( b \) is an ideal properly contained in \( S \) satisfying \( S \setminus b \subseteq p_1 \cup \cdots \cup p_n \), then \( S \) lies in one of the \( p_j \)'s.

Proof. Let \( m(\leq n) \) be the minimal number of \( a_i \)'s whose union contains \( S \). By reindexing if necessary, we can assume that \( S \subseteq a_1 \cup \cdots \cup a_m \) and \( S \nsubseteq \bigcup_{j \in J \subseteq \{1, 2, \ldots n\}} a_j \) if \( |J| < m \). Note that

\[
S = \bigcup_{i=1}^{m} (S \cap a_i) \quad \text{and} \quad \emptyset \neq S \cap a_i \nsubseteq \bigcup_{1 \leq j \leq m, j \neq i} a_j \quad \text{by the choice of } m.
\]

Choose \( a_i \in (S \cap a_i) \setminus \bigcup_{1 \leq j \leq m, j \neq i} a_j \). If \( m = 2 \), then we have \( a_1 + a_2 \in S \subseteq a_1 + a_2 \). If \( a_1 + a_2 \in a_1 \), then \( a_2 = (a_1 + a_2) - a_1 \in a_1 \), which is a contradiction. If \( a_1 + a_2 \not\subseteq a_2 \), we also get a contradiction.

If \( m \geq 3 \), then at least one of \( a_i \)'s, say \( a_1 \), is prime. Consider the element \( a = a_1 + a_2a_3 \cdots a_m \in S \subseteq a_1 \cup \cdots \cup a_m \). If \( a \in a_1 \), then \( a_2a_3 \cdots a_m = a - a_1 \in a_1 \). Since \( a_1 \) is prime, we have some \( a_j \in a_j \) for \( j \geq 2 \), which is a contradiction. If \( a \in a_j \) for some \( j \geq 2 \), then \( a_1 = a - (a_2 \cdots a_{j-1}a_j + 1 \cdots a_m)a_j \in a_j \), thus a contradiction.

This shows that \( m = 1 \), i.e., \( S \subseteq a_j \) for some \( j \). \( \square \)

**Problem** (25.21.2). Produce elements \( a \) and \( b \) in the domain \( R = \{ x + 2y\sqrt{-1} \mid x, y \in \mathbb{Z} \} \) having no gcd. Prove your elements do not have a gcd.

Proof. Consider \( a = 4 + 4i \) and \( b = 8 \) in \( R \). We can see that \( 2 \) and \( 2+2i \) are common divisors of \( a \) and \( b \). Note that \( N(x) \mid N(y) \) in \( \mathbb{Z} \) if \( x \mid y \) in \( R \), and there is no element having \( N(a) = 2 \) in \( R \) because \( N(x+2y\sqrt{-1}) = x^2 + 4y^2 = 2 \) has no solution in \( \mathbb{Z} \). Suppose there is a gcd \( g = (a, b) \) in \( R \).

\[
2, 2+2i \mid g \mid a, b
\]
gives us

\[
4, 8 \mid N(g) \mid N(a) = 32, N(b) = 64
\]
in \( \mathbb{Z} \). If \( N(g) = 8 \), then \( N(\frac{g}{2}) = 2 \). If \( N(g) = 16 \), then we have \( N(\frac{g}{2}) = 2 \). If \( N(g) = 32 \), then \( N(\frac{g}{2}) = 2 \). In all cases we end up getting elements in \( R \) with norms equal to 2, which is not possible. Therefore, \( a \) and \( b \) do not have a gcd in \( R \). \( \square \)

**Problem** (25.21.14). Prove that a domain in which every prime ideal is principal is a PID.
Proof. Let \( R \) be a domain satisfying the assumption,
\[
S = \{ a \subseteq R \mid a \text{ is an ideal which is not principal} \}
\]
and assume that \( S \) is nonempty. For any chain of ideals \( a_1 \subseteq a_2 \subseteq \cdots \) in \( S \), the union \( \bigcup_i a_i \) is not principal. (If \( \bigcup_i a_i = (a) \), then \( a \in a_j \) for some \( j \) and \( a_j = (a) \).) This means any chain in \( S \) has an upper bound in \( S \), so we can apply Zorn’s lemma to get a maximal element \( m \) in \( S \). Note that \( m \) is not prime by assumption, thus we have some \( a, b \in R \) such that \( a, b \notin m \) and \( ab \in m \). Since \( m + (a) \) is an ideal properly containing \( m, m + (a) = (c) \) for some \( c \in R \). Define the ideal quotient \( (m : (a)) = \{ r \in R \mid ra \in m \} \), then we can easily check that \( (m : (a)) \) is an ideal of \( R \) containing \( m + (b) \). Let \( (m : (a)) = (d) \) for \( d \in R \). Since \( da \in m \), we have
\[
(cy) \subseteq (m + (a))(d) \subseteq m
\]
On the other hand, for any \( x \in m \subseteq m + (a) = (c), x = cy \) for some \( y \in R \). Because \( a \in (c) \), we have \( ya \in (cy) \subseteq m \), which means \( y \in (m : (a)) = (d) \). Thus \( x \in (cd) \) and \( m \subseteq (cd) \). Therefore \( m = (cd) \) and this gives us a contradiction. So \( S \) is empty, and \( R \) is a PID.

**Problem (29.19.1).** Let \( R \) be a commutative ring. Show that a polynomial \( f = a_0 + a_1 t + \cdots + a_n t^n \) in \( R[t] \) is a unit in \( R[t] \) if and only if \( a_0 \) is a unit in \( R \) and \( a_i \) is nilpotent for every \( i > 0 \).

Proof. \(<\Rightarrow>\) Suppose \( a_0 \) is a unit and \( a_i \) is nilpotent for every \( i > 0 \). Consider \( g = a_0^{-1} f = 1 + \frac{a_1}{a_0} t + \cdots + \frac{a_n}{a_0} t^n \). Suppose we have \( a_i^{m_i} = 0 \), and let \( M = m_1 + \cdots + m_n \). Note that \( g - 1 \) is nilpotent in \( R[t] \) by
\[
(g - 1)^M = \left( \sum_{i=1}^{n} \frac{a_i}{a_0} t^i \right)^M = a_0^{-M} \sum_{r_1+r_2+\cdots+r_n=M} b_{r_1r_2\cdots r_n} a_1^{r_1} t^{r_1} = 0 \quad (b_{r_1r_2\cdots r_n} \in \mathbb{Z})
\]
because \( r_i \geq m_i \) for some \( i \). Thus, \( g = 1 + (g - 1) \in R[t]^\times \) (if \( u \in R[t] \) is nilpotent, then \( 1 + u \in R[t]^\times \); see [2], 23.16.4) and \( f = a_0 g \in R[t]^\times \).

\(<\Rightarrow>\) We give two solutions.

(Solution 1) We use induction on \( \deg f \). Suppose \( f(t)g(t) = 1 \) for some \( g(t) = b_0 + b_1 t + \cdots + b_m t^m \in R[t] \). By comparing the coefficients on both sides, we get
\[
a_n b_m = 0 \\
a_n b_{m-1} + a_{n-1} b_m = 0 \\
a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0 \\
\vdots \\
a_0 b_0 = 1
\]
The last equality \( a_0 b_0 = 1 \) shows that \( a_0 \) is a unit. Thus if \( \deg f = 0 \), then we’re done. Now we assume \( \deg f = n \geq 1 \). We multiply \( a_n \) on the second equality, then we get \( a_n^2 b_{m-1} = 0 \). If we multiply \( a_n^2 \) on the third equality, we get \( a_n^3 b_{m-2} = 0 \). In this way, we finally get \( a_n^{m+1} b_0 = 0 \). Since \( a_n^{m+1} = a_n^{m+1} b_0 a_0 = 0 \), \( a_n \) is nilpotent. Now we have \( g(t)(f(t) - a_n t^n) = 1 - g(t)a_n t^n \in R[t]^\times \) because \( g(t)a_n t^n \) is nilpotent. Thus \( f(t) - a_n t^n \) is also a unit with \( \deg f(t) - a_n t^n < n \). By the induction hypothesis, \( a_i \) is nilpotent for all \( 1 \leq i \leq n - 1 \).

(Solution 2) Let \( p \) be a prime ideal of \( R \) and consider the projection \( R[t] \to (R/p)[t] \). Note that \( R/p \) is a domain, and so is \( (R/p)[t] \). Thus if \( f \in R[t]^\times \), then \( f = f \mod p \in (R/p)[t]^\times = (R/p)^\times \).
This implies $a_i \in p$ for all $i > 0$ and all prime ideals $p$. Therefore

$$ a_i \in \bigcap_{p, \text{prime}} p = \text{nil}(R) $$

for all $i > 0$. (See [2], Cor 23.15) \hfill \square

**Problem (29.19.2).** Let $R$ be a nontrivial commutative ring and $f$ a zero divisor in $R[t]$. Show that there exists a nonzero element $b$ in $R$ so that $bf = 0$.

**Proof.** Write $f(t) = a_0 + a_1 t + \cdots + a_n t^n$. Let $g(t) = b_0 + b_1 t + \cdots + b_m t^m$ be a nonzero polynomial of minimal degree satisfying $gf = 0$. Suppose $m > 0$. If $ga_i = 0$ for all $0 \leq i \leq n$, then $b_m a_i = 0$ for all $i$ and we get $b_m f = 0$ which is a contradiction. Thus we can assume that there is a maximal $j \geq 0$ such that $ga_j \neq 0$. Now we have

$$ 0 = gf = (b_0 + b_1 t + \cdots + b_m t^m)(a_0 + a_1 t + \cdots + a_j t^j + a_{j+1} t^{j+1} + \cdots + a_n t^n) $$

$$ = (b_0 + b_1 t + \cdots + b_m t^m)(a_0 + a_1 t + \cdots + a_j t^j) $$

This means $a_j b_m = 0$ and $(a_j g)f = a_j(gf) = 0$. But $\deg a_j g < \deg g$ contradicts the minimality of $\deg g$. Therefore we have $m = 0$. \hfill \square

**Problem (38.23.6).** Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a $\mathbb{Z}$--module homomorphism. Let $S_l$ be the standard basis for $\mathbb{Z}$. Prove that $f$ is monic if and only if the rank of $[f]_{S_1}^{S_m}$ is $n$ and $f$ is epic if and only if a gcd of the $m$th ordered minors of $[f]_{S_1}^{S_m}$ is 1.

**Proof.** (Solution 1) We first prove this by using the following theorem.

(Theorem) Let $R$ be a PID and $A \in M_{m,n}(R)$. Then there are matrices $P \in GL_m(R), Q \in GL_n(R)$ such that $PAQ = \text{diag}(a_1, a_2, \cdots, a_r, 0, \cdots, 0)$ (called a Smith Normal Form of $A$) for $a_i \neq 0, a_1 | a_2 | \cdots | a_r$. Furthermore, the ideals $(a_1) \supset (a_2) \supset \cdots \supset (a_r)$ completely determine a Smith Normal Form of $A$ and $a_l \sim \Delta_l/\Delta_{l-1}$ where $\Delta_l = \Delta_{l,A}$ is a gcd of all $l \times l$ minors of $A$.

Let $A = [f]_{S_1}^{S_m}$. Then by the theorem above, we can find $P \in GL_m(\mathbb{Z}), Q \in GL_n(\mathbb{Z})$ such that $PAQ = \text{diag}(a_1, a_2, \cdots, a_r, 0, \cdots, 0)$. Clearly we have $r \leq \text{min}(m, n)$. We write $P = [id_{\mathbb{Z}^m}]_{S_1}^{S_m}$ and $Q = [id_{\mathbb{Z}^n}]_{\beta}^{\alpha}$ where $\alpha = \{v_1, v_2, \cdots, v_n\}$ and $\beta = \{w_1, w_2, \cdots, w_m\}$ are basis of $\mathbb{Z}^n$ and $\mathbb{Z}^m$ respectively. Now we have

$$ PAQ = [id_{\mathbb{Z}^m}]_{S_1}^{S_m}[f]_{S_1}^{S_m}[id_{\mathbb{Z}^n}]_{\alpha}^{\beta} = [id_{\mathbb{Z}^m} \circ f \circ id_{\mathbb{Z}^n}]_{\alpha}^{\beta} = [f]_{\alpha}^{\beta} = \text{diag}(a_1, \cdots, a_r, 0, \cdots, 0) $$

We can easily see that

$$ \ker f = \begin{cases} \mathbb{Z}v_{r+1} + \cdots + \mathbb{Z}v_n & \text{if } n > r \\ 0 & \text{if } n = r \end{cases} $$

and $\text{im } f = \mathbb{Z}a_1 w_1 + \cdots + \mathbb{Z}a_r w_r$ from $[f]_{\alpha}^{\beta}$. Now,

- $f$ is monic $\iff$ $\ker f = 0$ $\iff$ $r = n$ $\iff$ $\text{rank } f = n$ $\iff$ $\text{rank } [f]_{S_1}^{S_m} = n$
- $f$ is epic $\iff$ $\text{im } f = \mathbb{Z}a_1 w_1 + \cdots + \mathbb{Z}a_r w_r = \mathbb{Z}^m$ $\iff$ $r = m$ and $a_i = \pm 1$ for all $i$

$$ \iff \Delta_m [f]_{\alpha}^{\beta} = 1 $$

$$ \iff \Delta_m [f]_{S_1}^{S_m} = 1 $$

because $\Delta_m = a_1 a_2 \cdots a_m$ and $\Delta_l$ of similar matrices are associates for all $l$ by Lemma 37.6.
**Solution 2** Now we prove this without using a Smith Normal Form.

For the first part, let $S_n = \{e_1, e_2, \ldots, e_n\}$ and $S_m = \{f_1, f_2, \ldots, f_m\}$.

$f$ is monic $\iff$ ker $f = 0$ $\iff$ $f \left( \sum_{i=1}^{n} n_i e_i \right) = 0$ implies $n_i = 0$ for all $i$

$\iff$ $\sum_{i=1}^{n} n_i f(e_i) = 0$ implies $n_i = 0$ for all $i$

$\iff$ $\{f(e_i)\}_{i=1}^{n}$ is a basis of im $f$

$\iff$ rank$(f)_{S_n}^{S_m} = n$

For the second part, we first prove that if $f$ is epic, then $\Delta_m[f]_{S_n}^{S_m} = 1$. Let $A = [f]_{S_n}^{S_m}$. Since $f$ is surjective, we can find $v_1 = \left( \begin{array}{c} v_{11} \\ v_{12} \\ \vdots \\ v_{1m} \end{array} \right)$ such that $Av_1 = f_1$ for each $i$. Let $V$ be the $n \times m$ matrix whose $i$th column is $v_i$, then we have $AV = I_m$. We denote the $i$th column (resp. row) of $A$ by $[A]^i$ (resp. $[A]_i$). Using the fact that the determinant function is multilinear on columns, we can show that

$$1 = \det(I_m) = \det(v_{11}[A]^1 + \ldots + v_{1n}[A]^n, \ldots, v_{m1}[A]^1 + \ldots + v_{mn}[A]^n)$$

$$= v_{11}v_{21} \cdots v_{n1} \det([A]^1, [A]^1, \ldots, [A]^1) + \ldots + v_{1n}v_{2n} \cdots v_{mn} \det([A]^n, [A]^n, \ldots, [A]^n)$$

$$= \sum_{1 \leq i_1 < i_2 < \ldots < i_m \leq n} u_{i_1i_2\ldots i_m} \det([A]^{i_1}, \ldots, [A]^{i_m})$$

for some $u_{i_1i_2\ldots i_m} \in \mathbb{Z}$. We used the facts that the determinant of a matrix with two identical columns is zero, and that changing the order of columns only affects the sign of the determinant. The $m \times m$ minors of $A$ look like $([A]^{i_1} \cdots [A]^{i_m})$, thus the above equation says that $1$ is a $\mathbb{Z}$-linear combination of the determinants of $m \times m$ minors of $A$, i.e., $\Delta_m = 1$.

Finally, we prove that if $\Delta_m = 1$, then $f$ is epic. Since a gcd of the determinants of $m \times m$ minors of $A$ is 1, we can find integers $r_{i_1i_2\ldots i_m} \in \mathbb{Z}$ such that

$$1 = \sum_{1 \leq i_1 < i_2 < \ldots < i_m \leq n} r_{i_1i_2\ldots i_m} \det([A]^{i_1}, [A]^{i_2}, \ldots, [A]^{i_m})$$

Let $B_{i_1i_2\ldots i_m} = \text{adj}([A]^{i_1}[A]^{i_2} \cdots [A]^{i_m}) \in M_{m,m}(\mathbb{Z})$ and define $B_{\overline{i_1i_2\ldots i_m}} \in M_{n,m}(\mathbb{Z})$ by

$$[B_{\overline{i_1i_2\ldots i_m}}]_j = \begin{cases} [B_{i_1i_2\ldots i_m}]_k & \text{if } j = i_k \\ 0 & \text{otherwise} \end{cases}$$

Then we have $AB_{\overline{i_1i_2\ldots i_m}} = ([A]^{i_1} \cdots [A]^{i_m})B_{i_1i_2\ldots i_m} = \det([A]^{i_1} \cdots [A]^{i_m})I_m$. Because

$$A(\sum r_{i_1i_2\ldots i_m}B_{\overline{i_1i_2\ldots i_m}}) = (\sum r_{i_1i_2\ldots i_m} \det([A]^{i_1} \cdots [A]^{i_m}))I_m = I_m$$

is surjective, so is $A = [f]_{S_n}^{S_m}$.

\[ \square \]

**Problem (38.23.7).** Let $R$ be a commutative ring. Let $E_n(R)$ be the subgroup of $GL_n(R)$ generated by all matrices of the form $I + \lambda$ where $\lambda$ is a matrix with precisely one non-zero entry and this entry does not occur on the diagonal. Suppose that $R$ is a euclidean ring. Show that $SL_n(R) = E_n(R)$. 

16
Proof. We use induction on \( n \).
When \( n = 1 \), this is trivial because we have \( SL_1(R) = \{(1_R)\} = E_1(R) \).
Suppose \( n > 1 \). Note that every generator of \( E_n(R) \) has the form \( I + \lambda E_{ij} \) for some \( \lambda \in R \) and \( i \neq j \), thus has determinant 1. So it is clear that \( E_n(R) \subseteq SL_n(R) \).
Conversely, suppose \( A \in SL_n(R) \). For matrices \( M, N \in M_n(R) \), we write

\[
M \sim N \text{ if } N = PMQ \text{ for some } P, Q \in E_n(R)
\]

(\( \sim \) is an equivalence relation!) We will show that \( A \sim T \) for some \( T \in E_n(R) \), which implies that \( A \in E_n(R) \). We can also easily see that multiplying \( I + \lambda E_{ij} \) on the left is equivalent to adding \( \lambda \) times \( j \)-th row to \( i \)-th row, and multiplying \( I + \lambda E_{ij} \) on the right is equivalent to adding \( \lambda \) times \( i \)-th column to \( j \)-th column.
Since \( A = (a_{ij}) \neq 0 \), we can find a nonzero component \( a_{ij} \neq 0 \). We want to have \( a_{ij} | a_{ik}, a_{lj} \) for all \( 1 \leq k, l \leq n \). If this is not the case, pick \( a_{ik}(or a_{ij}) \) which is not divisible by \( a_{ij} \). Since \( R \) is a euclidean ring, we can find elements \( q, r \in R \) such that \( a_{ik}(or a_{ij}) = qa_{ij} + r \) with \( r \neq 0, \delta(r) < \delta(a_{ij}) \) where \( \delta \) is a euclidean function on \( R \). Now \( A(I - qE_{jk})(or (I - qE_{lk})A) \) has \( r \) as one of its entries. If \( r \) divides all entries on the same row/column, we’re good. Otherwise repeat the same process. This process has to stop after finite number of steps because we will have strictly decreasing values of \( \delta \), which is defined on \( \mathbb{Z}_{\geq 0} \).
Therefore we can assume that \( A \sim B = (b_{ij}) \) for some \( B \in SL_n(R) \) satisfying \( b_{ij} | b_{ik}, b_{lj} \) for some \( i, j \) and \( 1 \leq k, l \leq n \). Let \( b_{ik} = e_k b_{ij}, b_{lj} = f_l b_{ij} \) \((e_k, f_l \in R)\) and

\[
C = \left( \prod_{\substack{l \neq i \atop 1 \leq l \leq n}} (I - f_l E_{ik}) \right) B \left( \prod_{\substack{k \neq j \atop 1 \leq k \leq n}} (I - e_k E_{jk}) \right)
\]

then

\[
A \sim C = \begin{pmatrix}
0 & \cdots & * \\
\vdots & \ddots & \vdots & \ddots & *, \ldots & 0 \\
0 & \cdots & \cdots & 0 & b_{ij} & 0 & \cdots & 0 \\
0 & \cdots & \cdots & 0 & \cdots & 0 \\
0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 \\
0 & \cdots & \cdots & 0 & \cdots & \cdots & 0
\end{pmatrix}
\]

Also note that \( b_{ij} | \det C = \det A = 1 \), thus \( b_{ij} \in R^\times \). Let \( c_{11} \) be the \((1, 1)\)-th component of \( C \), and

\[
D = \begin{cases}
(I + E_{11})C(I + \frac{c_{11}}{b_{11}}E_{j1}) & \text{if } i \neq 1, j \neq 1 \\
C(I + \frac{1}{b_{1j}}E_{j1}) & \text{if } i = 1, j \neq 1 \\
(I + \frac{1}{b_{1j}}E_{j1})C & \text{if } i \neq 1, j = 1 \\
C & \text{if } i = j = 1
\end{cases}
\]

17
then
\[
A \sim D = (d_{ij}) = \left( \begin{array}{ccc}
1 & * \\
* & *
\end{array} \right) \sim \left( \prod_{2 \leq i \leq n} (I - d_{ii}E_{ii}) \right) D \left( \prod_{2 \leq k \leq n} (I - d_{1k}E_{1k}) \right) = \left( \begin{array}{cc}
1 & 0 \\
0 & A_1
\end{array} \right)
\]

for some \( A_1 \in SL_{n-1}(R) \). By inductive hypothesis, \( A_1 \in E_{n-1}(R) \), i.e., there are matrices \( U_1, U_2, \ldots, U_r \) such that \( U_k = I_{n-1} + \lambda_k E_{i_k,j_k} \) for some \( \lambda_k \in R, 1 \leq i_k, j_k \leq n-1 \) and \( A_1 = U_1 U_2 \cdots U_r \). Define
\[
V_k = \left( \begin{array}{cc}
1 & 0 \\
0 & U_k
\end{array} \right) = I_{n} + \lambda_k E_{i_k+1,j_k+1} \in E_n(R)
\]
then
\[
A \sim \left( \begin{array}{cc}
1 & 0 \\
0 & A_1
\end{array} \right) = V_1 V_2 \cdots V_r \in E_n(R)
\]

\[\square\]

**Problem (38.23.8).** Let \( A \) be a finite abelian group and let
\[
\hat{A} = \{ \chi : A \rightarrow \mathbb{C}^\times \mid \chi \text{ a group homomorphism} \}
\]
It is easily checked that \( \hat{A} \) is a group via \( \chi_1 \chi_2(x) = \chi_1(x) \chi_2(x) \). Show that

1. \( A \) and \( \hat{A} \) have the same order and, in fact, are isomorphic.
2. If \( \chi \) is not the identity element of \( \hat{A} \), then \( \sum_{a \in A} \chi(a) = 0 \).

**Proof.** (1) Suppose first \( A \) is cyclic and \( A \cong \mathbb{Z}/n\mathbb{Z} \). Define
\[
\phi : A \rightarrow \hat{A} = \text{Hom}(A, \mathbb{C}^\times) \\
\quad a \mapsto (\chi_a : b \mapsto \zeta_n \chi_a b)
\]
where \( \zeta_n = e^{2\pi i/n} \). \( \phi \) is a well-defined (\( \chi_a \in \hat{A} \) for all \( a \in A \)) group homomorphism. (\( \chi_{a+b} = \chi_a \chi_b \))
If \( \chi_a = 1_A \), then \( 1 = \chi_a(1) = \zeta_n, \) i.e., \( a = 0 \). Thus, \( \phi \) is injective.
For any \( \chi \in \hat{A}, 1 = \chi(0) = \chi(1)^n \). So \( \chi(1) = \zeta_k \) for some \( k \), and \( \chi = \chi_k \) because \( \chi(1) \) completely determines \( \chi \). Thus, \( \phi \) is surjective.
For a general finite abelian group \( A \), we know that \( A \cong \bigoplus_i A_i \) where \( A_i \)'s are cyclic groups.
Therefore, we have
\[
\hat{A} \cong \bigoplus_i \hat{A}_i \cong \prod_i \hat{A}_i \cong \prod_i A_i \cong A
\]
Note that the second isomorphism comes from a more general fact that \( \text{Hom}_R(\bigoplus_i A_i, B) \cong \prod_i \text{Hom}_R(A_i, B) \) (defined by \( f \mapsto (f \circ \iota_i) \) where \( \iota_i : A_i \hookrightarrow \bigoplus A_i \) for \( R \)-modules \( A_i, B \) and
any (possible infinite) index set \( I \). (Check this!)

(2) If \( \chi \neq 1_A \), then we can find \( b \in A \) such that \( \chi(b) \neq 1 \). We have

\[
(\chi(b) - 1) \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(b)\chi(a) - \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(a + b) - \sum_{a \in A} \chi(a) = 0
\]

Thus, \( \sum_{a \in A} \chi(a) = 0 \). \( \square \)

11. Some Examples

Example 11.1. Let \( R = \mathbb{Z}/6\mathbb{Z} \) and \( S = \{0, 3\} \subset R \). \( S \) itself is a ring, but is not a subring of \( R \) because \( 1_S = 3 \neq 1 = 1_R \). Note that \( 1_S = 3 \notin R^\times \).

Example 11.2. Let \( X \) be a set and \( \mathcal{P}(X) \) be the power set (the set of subsets) of \( X \). We define two operations \( +, \cdot \) on \( \mathcal{P}(X) \) by \( A + B = (A - B) \cup (B - A) = (A \cup B) \setminus (A \cap B) \) and \( A \cdot B = A \cap B \) for \( A, B \in \mathcal{P}(X) \). We can check that \( (\mathcal{P}(X), +, \cdot) \) is a ring with \( 0_{\mathcal{P}(X)} = \emptyset, 1_{\mathcal{P}(X)} = X \). Note that \( -A = A \) for \( A \in \mathcal{P}(X) \) and \( \mathcal{P}(X)^\times = \{X\} \).

Example 11.3. One good thing about Noetherian rings is that we don’t need Zorn’s lemma to have a maximal element in a set of ideals. However, when we prove that the ascending chain condition implies maximal principle, we still need Axiom of Choice (AC). In the proof, we construct a strictly ascending chain of ideals by assuming maximal principle doesn’t hold. Here we need Axiom of Dependent Choice (DC) to get an infinite sequence of ideals, and it is known that DC is not provable in ZF without AC. Induction is not enough because it only gives a finite chain.

Example 11.4. Let \( F \) be a field and consider an irreducible polynomial \( f \in F[t] \). If \( F \) is perfect (i.e., char \( F = 0 \) or char \( F = p \) and \( F = F^p \) for some prime \( p \)), then \( f' \neq 0 \).

Suppose \( f'(t) = 0 \). If char \( F = 0 \), then \( f' \neq 0 \) because otherwise \( f \) is a constant, which is a unit in \( F[t] \). If char \( F = p \), then there is \( g(t) = \sum_{i=0}^n b_it^i \in F[t] \) such that \( f(t) = g(t^p) \). Because \( F = F^p \), we can find \( a_i \in F \) such that \( a_i^p = b_i \) for all \( i \). Then, we have \( f(t) = \sum_{i=0}^n b_it^i = (\sum_{i=0}^n a_it^i)^p \), which contradicts the assumption that \( f \) is irreducible.

However, this can happen in general. Let \( F = F[y] \) where \( F \) is a finite field of order \( p \) and \( y \) is an indeterminate. Consider \( f(t) = t^p - y \in F[t] \). Note that \( y \) is prime in \( F[y] \), thus \( t^p - y \) is irreducible in \( (F[y])[t] \) by applying Eisenstein criterion with a prime \( y \in F[y] \). By Gauss lemma, it is also irreducible in \( \text{Frac}(F[y])[[t]] = (F[y])[t] \) where \( \text{Frac}(R) \) for a domain \( R \) means the quotient field of \( R \). But we have \( f'(t) = pt^{p-1} = 0 \) because \( \text{char} \ F[y] = p \).

Example 11.5. We have the following implications of properties of modules.

\[
\text{free} \implies \text{projective} \implies \text{flat} \implies \text{torsion-free}
\]

\( \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \) is a free \( \mathbb{Z}/6\mathbb{Z} \)-module, thus \( \mathbb{Z}/2\mathbb{Z} \) is projective but not free over \( \mathbb{Z}/6\mathbb{Z} \).

Let \( R = \mathbb{Z} \oplus \bigoplus_{i=1}^\infty \mathbb{Z}/2\mathbb{Z} \), then the principal ideal \( (2, 0)R \) is flat but not projective over \( R \).

Let \( k \) be a field and \( R = k[X, Y], I = (X, Y) \). Then \( I \) is torsion-free but not flat over \( R \).

A projective module over a local ring or a PID is free. A flat module over a perfect ring is projective. A torsion-free module over a Dedekind domain is flat.
References