20241129 MATH3301 NOTE 8[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

People study group G for the way $*$ it acts on set X. Useful though it is, we cannot even perform basic arithmetic on it, simply because there is only one operation, i.e, the group composition, on it. If we introduce two operations on a set R, and ensure that the two operations are compatible with each other, then we get the concept of ring.

2 Ring

2.1 Zero Ring, Ring with and without Unity

Definition 2.1. (**Ring**)
Let R be a nonempty set. If two binary operations $+ : R\times R \to R, * : R\times R \to R$, namely, addition and multiplication, are defined on R, and:
(1) For all $r, s \in R$:

$$r + s = s + r$$

(2) For all $r, s, t \in R$:

$$(r + s) + t = r + (s + t)$$

(3) For some zero element $0 \in R$, for all $r \in R$:

$$0 + r = r + 0 = r$$

(4) For all $r \in R$, for some negative element $-r \in R$:

$$(-r) + r = r + (-r) = 0$$

(5) For all $r, s, t \in R$:

$$(rs)t = r(st)$$

(6) For all $\lambda, r, s \in R$:

$$\lambda(r + s) = \lambda r + \lambda s \text{ and } (r + s)\lambda = r\lambda + s\lambda$$

If for some unity element $1 \in R$, for all $r \in R$:

$$1r = r1 = r$$

Then R is a ring with unity, otherwise R is a ring without unity.

Remark: *According to group theory, the zero element 0, the negative element $-r$, the unity element 1, and the reciprocal element r^{-1}, if they exist, are unique.*

Proposition 2.2. In a ring R with unity, $0 = 1$ iff $|R| = 1$.

Proof. We may divide our proof into two parts.
"if" direction: Assume that $|R| = 1$.

$$0 \in R \text{ and } 1 \in R \implies R = \{0\} \text{ and } R = \{1\} \implies 0 = 1$$

"only if" direction: Assume that $0 = 1$.

$$\forall r \in R, r = 1r = 0r = 0 \implies |R| = |\{0\}| = 1$$

Quod. Erat. Demonstrandum. □

Remark: *We define this ring as the zero ring.*

Example 2.3. $\mathbb{Z}$ is a nonzero ring under usual addition and multiplication.

Example 2.4. For all $n \geq 2$,
$\mathbb{Z}_n$ is a nonzero ring under congruence class addition and multiplication.

2.2 Ring Identifications

Definition 2.5. (**Ring Homomorphism**)
Let R, R' be two rings with unity, and $\sigma : R \to R'$ be a function. If:
(1) For all $r, s \in R$:

$$\sigma(r + s) = \sigma(r) + \sigma(s)$$

(2) For all $r, s \in R$:

$$\sigma(rs) = \sigma(r)\sigma(s)$$

(3) For the unity element $1 \in R$:

$$\sigma(1) = 1'$$

Then σ is a ring homomorphism.

Example 2.6. Define the followings:
(1) $\text{Obj} =$ [All rings with unity].
(2) $\text{Mor} =$ [All rings homomorphism].
(Obj, Mor) is a category.

Example 2.7. Let R be a commutative ring with unity. The function $\sigma : \mathbb{Z} \to R$, [The number n in $\mathbb{Z}$] $\mapsto$ [The number n in R] is a ring homomorphism.

Definition 2.8. (**Ring Isomorphism**)
Let R, R' be two rings with unity, and $\sigma : R \to R'$ be a ring homomorphism. If σ is bijective, then σ is a ring isomorphism, $R \cong R'$, i.e., R is isomorphic to R'.

Example 2.9. Define Obj = [All rings with unity].
$R \cong R'$ is an equivalence relation on Obj.

Proposition 2.10. For all $n \geq 2$, $\mathbb{Z}_n$ is not isomorphic to $\mathbb{Z}$.
For all distinct $n, m \geq 2$, $\mathbb{Z}_n$ is not isomorphic to $\mathbb{Z}_m$.

Proof. It suffices to notice that cardinality is invariant under ring isomorphism.
Quod. Erat. Demonstrandum. □

Definition 2.11. (**Two-sided Ideal**)
Let R be a ring with or without unity, and I be a subset of R. If:
(1) For the zero element $0 \in R$:

$$0 \in I$$

(2) For all $r, s \in R$:

$$r, s \in I \implies r + s \in I$$

(3) For all $r \in R$:

$$r \in I \implies -r \in I$$

(4) For all $\lambda, r \in R$:

$$r \in I \implies \lambda r, r\lambda \in I$$

Then I is a two-sided ideal of R.

Remark: *The zero ideal $\{0\}$ and the ring R are two-sided ideals of R.*
If we weaken (4) to $\lambda, r \in I \implies \lambda r \in I$, and force the unity 1 to lie in I, then we get the definition of subring.

Proposition 2.12. Let R, R' be two rings with unity,
and $\sigma : R \to R'$ be a ring homomorphism.
(1) If I is a two-sided ideal of R and σ is surjective,
then $\sigma(I)$ is a two-sided ideal of R'.
(2) If I' is a two-sided ideal of R',
then $\sigma^{-1}(I')$ is a two-sided ideal of R.

Proof. We may divide our proof into two parts.
Part 1: We prove that $\sigma(I)$ is a two-sided ideal of R'.

(1) Note that the element $\sigma(0) \in R'$ satisfies the following equation:

$$\sigma(0) + \sigma(0) = \sigma(0 + 0) = \sigma(0)$$

Hence, $0' = \sigma(0) \in \sigma(I)$.
(2) For all $r', s' \in \sigma(I)$, there exist $r, s \in I$,
such that $r' = \sigma(r)$ and $s' = \sigma(s)$, so:

$$r' + s' = \sigma(r) + \sigma(s) = \sigma(r + s) \in \sigma(I)$$

(3) For all $r' \in \sigma(I)$, there exists $r \in I$,
such that $r' = \sigma(r)$, so:

$$-r' = -\sigma(r) = \sigma(-r) \in \sigma(I)$$

(4) For all $\lambda' \in R' = \sigma(R)$ and $r \in \sigma(I)$, there exist $\lambda \in R$ and $r \in I$,
such that $\lambda' = \sigma(\lambda)$ and $r' = \sigma(r)$, so:

$$\begin{aligned} \lambda' r' &= \sigma(\lambda)\sigma(r) = \sigma(\lambda r) \in \sigma(I) \\ r'\lambda' &= \sigma(r)\sigma(\lambda) = \sigma(r\lambda) \in \sigma(I) \end{aligned}$$

Hence, $\sigma(I)$ is a two-sided ideal of R'.
Part 2: We prove that $\sigma^{-1}(I')$ is a two-sided ideal of R.
(1) Note that the element $\sigma(0) \in R'$ satisfies the following equation:

$$\sigma(0) + \sigma(0) = \sigma(0 + 0) = \sigma(0)$$

Hence, $0' = \sigma(0) \in I'$, $0 \in \sigma^{-1}(I')$.
(2) For all $r, s \in \sigma^{-1}(I')$:

$$\sigma(r + s) = \sigma(r) + \sigma(s) \in I' \implies r + s \in \sigma^{-1}(I')$$

(3) For all $r \in \sigma^{-1}(I')$:

$$\sigma(-r) = -\sigma(r) \in I' \implies -r \in \sigma^{-1}(I')$$

(4) For all $\lambda \in R$ and $r \in \sigma^{-1}(I')$:

$$\begin{aligned} \sigma(\lambda r) &= \sigma(\lambda)\sigma(r) \in I' \implies \lambda r \in \sigma^{-1}(I') \\ \sigma(r\lambda) &= \sigma(r)\sigma(\lambda) \in I' \implies r\lambda \in \sigma^{-1}(I') \end{aligned}$$

Hence, $\sigma^{-1}(I')$ is a two-sided ideal of R.
Quod. Erat. Demonstrandum. □

Example 2.13. For all $n \geq 2$, $n\mathbb{Z}$ is a nonzero proper two-sided ideal of $\mathbb{Z}$.

Proposition 2.14. For all nonzero proper two-sided ideal I of $\mathbb{Z}$, there exists a unique $n \geq 2$, such that $I = n\mathbb{Z}$.

Proof. Construct the following subset of $\mathbb{Z}$:

$$N = \{|n| \in \mathbb{Z} : n \in I \backslash \{0\}\}$$

As I is not the zero ideal $\{0\}$, N is nonempty.
As I is not R, N has a lower bound 2.
According to well-ordering principle, N has a unique minimum $n \geq 2$.
As I is closed under negative element, n must be an element of I, so $n\mathbb{Z} \subseteq I$.
Assume to the contrary that some m in I is not in $n\mathbb{Z}$.
According to the division algorithm, there exists a unique pair $q, r \in \mathbb{Z}$, such that:

$$m = qn + r, 0 < r < n$$

It follows that N contains a smaller element $0 < r = m + (-q)n < n$, which contradicts to the minimality of n.
Hence, our assumption is false, and we've proven that $n\mathbb{Z} = I$.
Quod. Erat. Demonstrandum. □

Definition 2.15. (**Kernel**)
Let R, R' be two rings with unity, and $\sigma : R \to R'$ be a ring homomorphism.
Define $\text{Ker}(\sigma) = \sigma^{-1}(\{0'\})$ as the kernel of σ.

Remark: *It follows that* $\text{Ker}(\sigma)$ *is always a two-sided ideal of* R*.*

Definition 2.16. (**Ring Characteristic**)
Let R be a ring with unity, and $\sigma : \mathbb{Z} \to R, [\text{The number } n \text{ in } \mathbb{Z}] \mapsto [\text{The number } n \text{ in } R]$ be the ring homomorphism constructed in **Example 2.7.**.
There exists a unique $n \geq 0$, such that the two-sided ideal $\text{Ker}(\sigma) = n\mathbb{Z}$.
Define this $n \geq 0$ as the characteristic $\text{Char}(R)$ of R.

Remark: *Ring characteristic is invariant under ring isomorphism.*

2.3 Ring Constructions

Proposition 2.17. Let R be a ring without unity.
Define $\mathbb{Z} \oplus R$ as the set of all expressions in the form [The number m in $\mathbb{Z}$] $\oplus$ [The element r in R], and $+$ and multiplication $*$ by:

$$\begin{aligned}(m \oplus r) + (n \oplus s) &= m + n \oplus r + s \\ (m \oplus r)(n \oplus s) &= mn \oplus ms + nr + rs\end{aligned}$$

$\mathbb{Z} \oplus R$ is a ring with unity, and $0 \oplus R$ is a two-sided ideal of $\mathbb{Z} \oplus R$.

Proof. We may divide our proof into two parts.
Part 1: In this part, we prove that $\mathbb{Z} \oplus R$ is a ring with unity.
(1) For all $m \oplus r, n \oplus s \in \mathbb{Z} \oplus R$:

$$\begin{aligned}(m \oplus r) + (n \oplus s) &= m + n \oplus r + s \\ &= n + m \oplus s + r \\ &= (n \oplus s) + (m \oplus r)\end{aligned}$$

(2) For all $m \oplus r, n \oplus s, k \oplus t \in \mathbb{Z} \oplus R$:

$$\begin{aligned}[(m \oplus r) + (n \oplus s)] + (k \oplus t) &= (m + n \oplus r + s) + (k \oplus t) \\ &= (m + n) + k \oplus (r + s) + t \\ &= m + (n + k) \oplus r + (s + t) \\ &= (m \oplus r) + (n + k \oplus s + t) \\ &= (m \oplus r) + [(n \oplus s) + (k \oplus t)]\end{aligned}$$

(3) For some zero element $0 \oplus 0 \in \mathbb{Z} \oplus R$, for all $m \oplus r \in \mathbb{Z} \oplus R$:

$$\begin{aligned}(0 \oplus 0) + (m \oplus r) = 0 + m \oplus 0 + r = m \oplus r \\ (m \oplus r) + (0 \oplus 0) = m + 0 \oplus r + 0 = m \oplus r\end{aligned}$$

(4) For all $m \oplus r \in \mathbb{Z} \oplus R$, for some negative element $-m \oplus -r \in \mathbb{Z} \oplus R$:

$$\begin{aligned}(-m \oplus -r) + (m \oplus r) = (-m) + m \oplus (-r) + r = 0 \oplus 0 \\ (m \oplus r) + (-m \oplus -r) = m + (-m) \oplus r + (-r) = 0 \oplus 0\end{aligned}$$

(5) For all $m \oplus r, n \oplus s, k \oplus t \in \mathbb{Z} \oplus R$:

$$\begin{aligned}[(m \oplus r)(n \oplus s)](k \oplus t) &= (mn \oplus ms + nr + rs)(k \oplus t) \\ &= mnk \oplus mks + nkr + mnt + mst + nrt + krs + rst \\ &= (m \oplus r)(nk \oplus nt + ks + st) \\ &= (m \oplus r)[(n \oplus s)(k \oplus t)]\end{aligned}$$

(6) For some unity element $1 \oplus 0 \in \mathbb{Z} \oplus R$, for all $m \oplus r \in \mathbb{Z} \oplus R$:

$$\begin{aligned}(1 \oplus 0)(m \oplus r) &= 1m \oplus 1r + m0 + 0r = m \oplus r\\ (m \oplus r)(1 \oplus 0) &= m1 \oplus m0 + 1r + r0 = m \oplus r\end{aligned}$$

(7) For all $l \oplus \lambda, m \oplus r, n \oplus s \in \mathbb{Z} \oplus R$:

$$\begin{aligned}(l \oplus \lambda)[(m \oplus r) + (n \oplus s)] &= (l \oplus \lambda)(m + n \oplus r + s)\\ &= l(m+n) \oplus l(r+s) + (m+n)\lambda + \lambda(r+s)\\ &= lm + ln \oplus (lr + m\lambda + \lambda r) + (ls + n\lambda + \lambda s)\\ &= (lm \oplus lr + m\lambda + \lambda r) + (ln \oplus ls + n\lambda + \lambda s)\\ &= (l \oplus \lambda)(m \oplus r) + (l \oplus \lambda)(n \oplus s)\\ [(m \oplus r) + (n \oplus s)](l \oplus \lambda) &= (m + n \oplus r + s)(l \oplus \lambda)\\ &= (m+n)l \oplus (m+n)\lambda + l(r+s) + (r+s)\lambda\\ &= ml + nl \oplus (m\lambda + lr + r\lambda) + (n\lambda + ls + s\lambda)\\ &= (ml \oplus m\lambda + lr + r\lambda) + (nl \oplus n\lambda + ls + s\lambda)\\ &= (m \oplus r)(l \oplus \lambda) + (n \oplus s)(l \oplus \lambda)\end{aligned}$$

Hence, $\mathbb{Z} \oplus R$ is a ring with unity.
Part 2: In this part, we prove that $0 \oplus R$ is a two-sided ideal of $\mathbb{Z} \oplus R$.
(1) For the zero element $0 \oplus 0 \in \mathbb{Z} \oplus R$:

$$0 \oplus 0 \in 0 \oplus R$$

(2) For all $0 \oplus r, 0 \oplus s \in 0 \oplus R$:

$$(0 \oplus r) + (0 \oplus s) = 0 + 0 \oplus r + s = 0 \oplus r + s \in 0 \oplus R$$

(3) For all $0 \oplus r \in 0 \oplus R$:

$$-(0 \oplus r) = -0 \oplus -r = 0 \oplus -r \in 0 \oplus R$$

(4) For all $l \oplus \lambda \in \mathbb{Z} \oplus R$ and $0 \oplus r \in 0 \oplus R$:

$$\begin{aligned}(l \oplus \lambda)(0 \oplus r) &= l0 \oplus lr + 0\lambda + \lambda r = 0 \oplus (l + \lambda)r \in 0 \oplus R\\ (0 \oplus r)(l \oplus \lambda) &= 0l \oplus 0\lambda + lr + r\lambda = 0 \oplus r(l + \lambda) \in 0 \oplus R\end{aligned}$$

Hence, $0 \oplus R$ is a two-sided ideal of $\mathbb{Z} \oplus R$.
Quod. Erat. Demonstrandum. □

Remark: *Now every ring has an ambient ring with unity.*

Example 2.18. Let R be a ring with unity, and X be a nonempty subset of R. The following subset of R is a two-sided ideal of R:

$$RXR = \left\{ \sum_{\mu \in U} r_\mu x_\mu s_\mu \in R : \text{each } r_\mu \in R \text{ and } x_\mu \in X \text{ and } s_\mu \in R \right\}$$

Example 2.19. Let R be a ring with unity, and $(I_\lambda)_{\lambda \in \Lambda}$ be an indexed family of two-sided ideals of R. The following subset of R is a two-sided ideal of R:

$$\bigcap_{\lambda \in \Lambda} I_\lambda = \{ r \in R : r \text{ is in each } I_\mu \}$$

Example 2.20. Let R be a ring with unity, and $(I_\lambda)_{\lambda \in \Lambda}$ be an indexed family of two-sided ideals of R. The following subset of R is a two-sided ideal of R:

$$\sum_{\lambda \in \Lambda} I_\lambda = R \{ r \in R : r \text{ is in some } I_\mu \} R$$

Example 2.21. Let R be a ring with unity, and $(I_k)_{k=1}^{m}$ be a finite list of two sided ideals of R. The following subset of R is a two-sided ideal of R:

$$\prod_{k=1}^{m} I_k = R \left\{ \prod_{k=1}^{m} r_k \in R : \text{each } r_k \in I_k \right\} R$$

Example 2.22. Let $(R_\lambda)_{\lambda \in \Lambda}$ be an indexed family of rings with unity.
(1) The Cartesian product $R = \prod_{\lambda \in I} R_\lambda$ is a ring with unity.
(2) For all subset I of R, I is a two-sided ideal of R
iff each $I_\mu = \pi_\mu(I)$ is a two-sided ideal of R_μ, and $I = \prod_{\lambda \in I} I_\lambda$.
Here, each $\pi_\mu : R \to R_\mu, r \mapsto r(\mu)$ is a natural projection.

Remark: *Notice that* $\mathbb{Z}[\mathrm{i}]$ *is isomorphic to* $\mathbb{Z} \times \mathbb{Z}$ *as a group, but not as a ring.*

Proposition 2.23. Let R be a ring with unity, and I be a two-sided ideal of R. Define $R/I = \{ r + I \subseteq R : r \in R \}$, and addition $+$ and multiplication $*$ by:

$$(r+I)+(s+I) = r+s+I$$
$$(r+I)(s+I) = rs+I$$

R/I is a ring with unity, $\pi : R \to R/I, r \mapsto r + I$ is a surjective ring homomorphism, and $\mathrm{Ker}(\pi) = I$.

Proof. We may divide our proof into four parts.
Part 1: We prove that the addition $+$ and multiplication $*$ are well-defined.
(1) For all $r_1 + I, r_2 + I, s_1 + I, s_2 + I \in R/I$:

$$\begin{aligned} r_1 + I = r_2 + I \text{ and } s_1 + I = s_2 + I &\implies \exists r, s \in I, r_1 = r_2 + r \text{ and } s_1 = s_2 + s \\ &\implies \exists t = r + s \in I, r_1 + s_1 = r_2 + s_2 + t \\ &\implies r_1 + s_1 + I = r_2 + s_2 + I \end{aligned}$$

Hence, the addition $+$ is well-defined.
(2) For all $r_1 + I, r_2 + I, s_1 + I, s_2 + I \in R/I$:

$$\begin{aligned} r_1 + I = r_2 + I \text{ and } s_1 + I = s_2 + I &\implies \exists r, s \in I, r_1 = r_2 + r \text{ and } s_1 = s_2 + s \\ &\implies \exists t = rs_2 + r_2 s + rs \in R, r_1 s_1 = r_2 s_2 + t \\ &\implies r_1 s_1 + I = r_2 s_2 + I \end{aligned}$$

Hence, the multiplication $*$ is well-defined.
Part 2: We prove that R/I is a ring with unity.
(1) For all $r + I, s + I \in R/I$:

$$\begin{aligned} (r + I) + (s + I) &= r + s + I \\ &= s + r + I \\ &= (s + I) + (r + I) \end{aligned}$$

(2) For all $r + I, s + I, t + I \in R/I$:

$$\begin{aligned} [(r + I) + (s + I)] + (t + I) &= (r + s + I) + (t + I) \\ &= (r + s) + t + I \\ &= r + (s + t) + I \\ &= (r + I) + (s + t + I) \\ &= (r + I) + [(s + I) + (t + I)] \end{aligned}$$

(3) For some zero element $0 + I \in R/I$, for all $r + I \in R/I$:

$$\begin{aligned} (0 + I) + (r + I) = 0 + r + I = r + I \\ (r + I) + (0 + I) = r + 0 + I = r + I \end{aligned}$$

(4) For all $r + I \in R/I$, for some negative element $-r + I \in R/I$:

$$\begin{aligned} (-r + I) + (r + I) = (-r) + r + I = 0 + I \\ (r + I) + (-r + I) = r + (-r) + I = 0 + I \end{aligned}$$

(5) For all $r+I, s+I, t+I \in R/I$:

$$\begin{aligned}[(r+I)(s+I)](t+I) &= (rs+I)(t+I)\\ &= (rs)t+I\\ &= r(st)+I\\ &= (r+I)(st+I)\\ &= (r+I)[(s+I)(t+I)]\end{aligned}$$

(6) For some unity element $1+I \in R/I$, for all $r+I \in R/I$:

$$\begin{aligned}(1+I)(r+I) &= 1r+I = r+I\\ (r+I)(1+I) &= r1+I = r+I\end{aligned}$$

(7) For all $\lambda+I, r+I, s+I \in R/I$:

$$\begin{aligned}(\lambda+I)[(r+I)+(s+I)] &= (\lambda+I)(r+s+I)\\ &= \lambda(r+s)+I\\ &= \lambda r+\lambda s+I\\ &= (\lambda r+I)+(\lambda s+I)\\ &= (\lambda+I)(r+I)+(\lambda+I)(s+I)\\ [(r+I)+(s+I)](\lambda+I) &= (r+s+I)(\lambda+I)\\ &= (r+s)\lambda+I\\ &= r\lambda+s\lambda+I\\ &= (r\lambda+I)+(s\lambda+I)\\ &= (r+I)(\lambda+I)+(s+I)(\lambda+I)\end{aligned}$$

Hence, R/I is a ring with unity.
Part 3: We prove that π is a surjective ring homomorphism.
(1) Every $r+I \in R/I$ is the image of some $r \in R$ under π.
(2) For all $r, s \in R$:

$$\begin{aligned}\pi(r+s) &= r+s+I\\ &= (r+I)+(s+I)\\ &= \pi(r)+\pi(s)\end{aligned}$$

(3) For all $r, s \in R$:

$$\begin{aligned}\pi(rs) &= rs+I\\ &= (r+I)(s+I)\\ &= \pi(r)+\pi(s)\end{aligned}$$

(4) For the unity element $1 \in R$, $\pi(1) = 1 + I$ is the unity of R/I.
Hence, π is a surjective ring homomorphism.
Part 4: We prove that $\mathrm{Ker}(\pi) = I$.

$$\begin{aligned}\mathrm{Ker}(\pi) &= \pi^{-1}(\{0+I\}) \\ &= \{r \in R : \pi(r) \in \{0+I\}\} \\ &= \{r \in R : r + I = 0 + I\} \\ &= I\end{aligned}$$

Quod. Erat. Demonstrandum. □

Remark: *When handling expressions like $(r+I)(s+I)$, we always follow the same procedure described in* ***Example 2.20.*** *to make it closed under addition.*

Theorem 2.24. (**The First Ring Isomorphism Theorem**)
Let R, R' be two rings with unity, and $\sigma : R \to R'$ be a surjective ring homomorphism. The quotient map $\widetilde{\sigma} : \widetilde{R} \to R', \widetilde{\sigma}(\widetilde{r}) = \sigma(r)$ is a ring isomorphism, where $\widetilde{R} = R/\mathrm{Ker}(\sigma)$ and $\widetilde{r} = r + I$.

Proof. We may divide our proof into three parts.
Part 1: We prove that $\widetilde{\sigma}$ is well-defined.
For all $\widetilde{r} \in \widetilde{R}$:

$$\begin{aligned}\widetilde{r} = \widetilde{0} &\implies r \in \mathrm{Ker}(\sigma) \\ &\implies \sigma(r) = \sigma(0) = 0'\end{aligned}$$

Hence, $\widetilde{\sigma}$ is well-defined.
Part 2: We prove that $\widetilde{\sigma}$ is bijective.
(1) For all $\widetilde{r} \in \widetilde{R}$:

$$\begin{aligned}\sigma(r) = 0' &\implies r \in \mathrm{Ker}(\sigma) \\ &\implies \widetilde{r} = \widetilde{0}\end{aligned}$$

(2) For all $r' \in R'$:

$$\exists r \in R, r' = \sigma(r) \implies \exists \widetilde{r} \in \widetilde{R}, r' = \widetilde{\sigma}(\widetilde{r})$$

Hence, $\widetilde{\sigma}$ is bijective.
Part 3: We prove that $\widetilde{\sigma}$ is a ring homomorphism.

(1) For all $\widetilde{r}, \widetilde{s} \in \widetilde{R}$:

$$\begin{aligned}
\widetilde{\sigma}(\widetilde{r} + \widetilde{s}) &= \widetilde{\sigma}(\widetilde{r + s}) \\
&= \sigma(r + s) \\
&= \sigma(r) + \sigma(s) \\
&= \widetilde{\sigma}(\widetilde{r}) + \widetilde{\sigma}(\widetilde{s})
\end{aligned}$$

(2) For all $\widetilde{r}, \widetilde{s} \in \widetilde{R}$:

$$\begin{aligned}
\widetilde{\sigma}(\widetilde{r}\widetilde{s}) &= \widetilde{\sigma}(\widetilde{rs}) \\
&= \sigma(rs) \\
&= \sigma(r)\sigma(s) \\
&= \widetilde{\sigma}(\widetilde{r})\widetilde{\sigma}(\widetilde{s})
\end{aligned}$$

(3) For the unity element $\widetilde{1} \in \widetilde{R}$:

$$\begin{aligned}
\widetilde{\sigma}(\widetilde{1}) &= \sigma(1) \\
&= 1'
\end{aligned}$$

To conclude, $\widetilde{\sigma}$ is a ring isomorphism. Quod. Erat. Demonstrandum. □

Theorem 2.25. (**The Second Ring Isomorphism Theorem**)
Let R be a ring with unity, S be a subring of R,
and I be a two-sided ideal of R.
The quotient map $\widetilde{\sigma} : S/(S \cap I) \to (S + I)/I$,
$r + (S \cap I) \mapsto r + I$ is a ring isomorphism.

Proof. We may divide our proof into three parts.
Part 1: We prove that $\sigma : S \to (S + I)/I, r \mapsto r + I$ is surjective.
For all $r + I \in (S + I)/I$, $r + I$ is the image of some $r \in S + I$ under σ.
Write $r \in S + I$ as $r = s + i$, where $s \in S$ and $i \in I$.
For some $s \in S$, $\sigma(s) = s + I = s + i + I = r + I$, so σ is surjective.
Part 2: We prove that $\sigma : S \to (S + I)/I, r \mapsto r + I$ is a ring homomorphism.
(1) For all $r, s \in S$:

$$\begin{aligned}
\sigma(r + s) &= r + s + I \\
&= (r + I) + (s + I) \\
&= \sigma(r) + \sigma(s)
\end{aligned}$$

(2) For all $r, s \in S$:

$$\begin{aligned}\sigma(rs) &= rs + I \\ &= (r+I)(s+I) \\ &= \sigma(r)\sigma(s)\end{aligned}$$

(3) For the unity element $1 \in S$:

$$\sigma(1) = 1 + I$$

Part 3: We prove that $\mathrm{Ker}(\sigma) = S \cap I$.

$$\begin{aligned}\mathrm{Ker}(\sigma) &= \sigma^{-1}(\{0+I\}) \\ &= \{r \in S : r + I \in \{0+I\}\} \\ &= S \cap I\end{aligned}$$

According to **Theorem 2.24.**, $\widetilde{\sigma} : S/(S\cap I) = S/\mathrm{Ker}(\sigma) \to (S+I)/I, r+(S\cap I) \mapsto r+I$ is a ring isomorphism. Quod. Erat. Demonstrandum. □

Theorem 2.26. (**The Third Ring Isomorphism Theorem**)
Let R be a ring with unity,
and I, K be two two-sided ideals of R with $K \subseteq I$.
The quotient map $\widetilde{\sigma} : (R/K)/(I/K) \to R/I$,
$(r+K) + I/K \mapsto r + I$ is a ring isomorphism.

Proof. We may divide our proof into four parts.
Part 1: We prove that $\sigma : R/K \to R/I, r + K \mapsto r + I$ is well-defined.
For all $r + K, s + K \in R/K$:

$$\begin{aligned}r + K = s + K &\implies \exists t \in K, r = s + t \\ &\implies \exists t \in I, r = s + t \\ &\implies r + I = s + I\end{aligned}$$

Hence, σ is well-defined.
Part 2: We prove that $\sigma : R/K \to R/I, r + K \mapsto r + I$ is surjective.
For all $r + I \in R/I$, for some $r + K \in R/K$, $\sigma(r + K) = r + I$.
Hence, σ is well-defined.
Part 3: We prove that $\sigma : R/K \to R/I, r + K \mapsto r + I$ is a ring homomorphism.

(1) For all $r+K, s+K \in R/K$:

$$\begin{aligned}\sigma((r+K)+(s+K)) &= \sigma(r+s+K)\\ &= r+s+I\\ &= (r+I)+(s+I)\\ &= \sigma(r+K)+\sigma(s+K)\end{aligned}$$

(2) For all $r+K, s+K \in R/K$:

$$\begin{aligned}\sigma((r+K)(s+K)) &= \sigma(rs+K)\\ &= rs+I\\ &= (r+I)(s+I)\\ &= \sigma(r+K)\sigma(s+K)\end{aligned}$$

(3) For the unity element $1+K \in R/K$:

$$\sigma(1+K) = 1+I$$

Part 4: We prove that $\mathrm{Ker}(\sigma) = I/K$.

$$\begin{aligned}\mathrm{Ker}(\sigma) &= \sigma^{-1}(\{0+I\})\\ &= \{r+K \in R/K : r+I \in \{0+I\}\}\\ &= I/K\end{aligned}$$

According to **Theorem 2.24.**, $\widetilde{\sigma} : (R/K)/(I/K) = (R/K)/\mathrm{Ker}(\sigma) \to R/I, (r+K)+I/K \mapsto r+I$ is a ring isomorphism. Quod. Erat. Demonstrandum. □

2.4 Field and Integral Domain

Definition 2.27. (**Unit**)
Let R be a ring with unity, and r be an element of R.
If there exists $s \in R$, such that $rs = sr = 1$, then r is a unit.

Example 2.28. Let R be a ring with unity.
The set $R^\times$ of all units of R forms a group under multiplication.

Definition 2.29. (**Field**)
Let R be a ring with unity. If R is nonzero and commutative,
and every nonzero element is a unit, then R is a field.

Example 2.30. $\mathbb{Z}$ is not a field, but $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example 2.31. For all $n \geq 2$, $\mathbb{Z}_n$ is a field iff n is prime.

Proposition 2.32. Let R be a ring with unity.
For all two-sided ideal I of R, if I contains a unit, then $I = R$.

Proof. For all ideal I of R, assume that I contains a unit r.
As there exists $s \in R$, such that $1 = sr \in I$, it follows that every $t \in R$ is actually an element $t = t1$ of I, so $I = R$. Quod. Erat. Demonstrandum. □

Remark: *Studying ideals of a field is not the correct way to understand it.*

Definition 2.33. (**Zero Divisor**)
Let R be a ring with unity, and r be an element of R.
(1) If r is nonzero, and there exists a nonzero element s of R,
such that $sr = 0$ or $rs = 0$, then r is a zero divisor.
(2) If r is nonzero, and there exists a nonzero element s of R,
such that $sr = 0$ and $rs = 0$, then r is a two-sided zero divisor.

Proposition 2.34. Let R be a ring with unity, and r be an element of R.
If r is a zero divisor, then r is not a unit.

Proof. WLOG, assume that $r \neq 0$ and for some nonzero element s of R, $rs = 0$.
Assume to the contrary that r is also a unit, so for some $t \in R$, $tr = rt = 1$.
Now $s = 1s = trs = t0 = 0$, contradicting to $s \neq 0$. Hence, our assumption is false, and we've proven that r is not a unit. Quod. Erat. Demonstrandum. □

Definition 2.35. (**Integral Domain**)
Let R be a ring with unity. If R is nonzero and commutative,
and R has no zero divisor, then R is an integral domain.

Remark: *As we wished, $\mathbb{Z}$ is an integral domain.*

Proposition 2.36. If R is a finite integral domain, then R is a field.

Proof. Assume to the contrary that $R = \{r_0 = 0, r_1 = 1, r_2, \cdots, r_n\}$ is not a field but an integral domain. For some nonzero element r_k of R, for all $r_l \in R$, $r_k r_l \neq 1$.
As R is an integral domain, $r_k r_1, r_k r_2, \cdots, r_k r_n \in \{r_2, r_3, \cdots, r_n\}$.
According to pigeon hole principle, there exists a distinct pair of integers $1 \leq s < t \leq n$, such that $r_k r_s = r_k r_t$, so $r_k(r_s - r_t) = 0$, where both r_k and $r_s - r_t$ are nonzero.
This contradicts to our assumption that R is an integral domain.
Hence, R must be a field. Quod. Erat. Demonstrandum. □

Remark: *As a consequence, $\mathbb{Z}_n$ is an integral domain iff n is prime.*

3 Noncommutative Ring

3.1 Abelian Group Homomorphism Ring

Proposition 3.1. Let G be an Abelian group, and $\mathrm{Mor}(G,G)$ be the set of all group homomorphisms on G. Define addition $+$ and multiplication $*$ by:

$$\begin{aligned} g \mapsto \mu(g) + g \mapsto \nu(g) = g \mapsto \mu(g) + \nu(g) \\ g \mapsto \mu(g) * g \mapsto \nu(g) = g \mapsto \mu\nu(g) \end{aligned}$$

$\mathrm{Mor}(G,G)$ is a ring with unity. If $\sigma : G \to G'$ is a group isomorphism, then $c_\sigma : \mathrm{Mor}(G,G) \to \mathrm{Mor}(G',G'), \tau \mapsto \sigma\tau\sigma^{-1}$ is a ring isomorphism.

Proof. We may divide our proof into three parts.
Part 1: We prove that the addition $+$ and multiplication $*$ are well-defined.
(1) For all $\mu, \nu \in \mathrm{Mor}(G,G)$, we wish to show that $\mu + \nu \in \mathrm{Mor}(G,G)$.
For all $g, h \in G$:

$$\begin{aligned} (\mu+\nu)(g+h) &= \mu(g+h) + \nu(g+h) \\ &= \mu(g) + \mu(h) + \nu(g) + \nu(h) \\ &= \mu(g) + \nu(g) + \mu(h) + \nu(h) \\ &= (\mu+\nu)(g) + (\mu+\nu)(h) \end{aligned}$$

Hence, $\mu + \nu \in \mathrm{Mor}(G,G)$, the addition $+$ is well-defined.
Similarly, $0, -\mu \in \mathrm{Mor}(G,G)$ are well-defined.
(2) For all $\mu, \nu \in \mathrm{Mor}(G,G)$, we wish to show that $\mu\nu \in \mathrm{Mor}(G,G)$.
For all $g, h \in G$:

$$\begin{aligned} \mu\nu(g+h) &= \mu(\nu(g) + \nu(h)) \\ &= \mu\nu(g) + \mu\nu(h) \end{aligned}$$

Hence, $\mu\nu \in \mathrm{Mor}(G,G)$, the multiplication $*$ is well-defined.
Similarly, $e_G \in \mathrm{Mor}(G,G)$ is well-defined.
Part 2: We prove that $\mathrm{Mor}(G,G)$ is a ring with unity.
(1) For all $g \mapsto \mu(g), g \mapsto \nu(g) \in \mathrm{Mor}(G,G)$:

$$\begin{aligned} g \mapsto \mu(g) + g \mapsto \nu(g) &= g \mapsto \mu(g) + \nu(g) \\ &= g \mapsto \nu(g) + \mu(g) \\ &= g \mapsto \nu(g) + g \mapsto \mu(g) \end{aligned}$$

(2) For all $g \mapsto \mu(g), g \mapsto \nu(g), g \mapsto \sigma(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
[g \mapsto \mu(g) + g \mapsto \nu(g)] + g \mapsto \sigma(g) &= g \mapsto \mu(g) + \nu(g) + g \mapsto \sigma(g) \\
&= g \mapsto [\mu(g) + \nu(g)] + \sigma(g) \\
&= g \mapsto \mu(g) + [\nu(g) + \sigma(g)] \\
&= g \mapsto \mu(g) + g \mapsto \nu(g) + \sigma(g) \\
&= g \mapsto \mu(g) + [g \mapsto \nu(g) + g \mapsto \sigma(g)]
\end{aligned}$$

(3) For some zero element $g \mapsto 0 \in \mathrm{Mor}(G, G)$, for all $g \mapsto \mu(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
g \mapsto 0 + g \mapsto \mu(g) = g \mapsto 0 + \mu(g) = g \mapsto \mu(g) \\
g \mapsto \mu(g) + g \mapsto 0 = g \mapsto \mu(g) + 0 = g \mapsto \mu(g)
\end{aligned}$$

(4) For all $g \mapsto \mu(g) \in \mathrm{Mor}(G, G)$, for some negative element $g \mapsto -\mu(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
g \mapsto -\mu(g) + g \mapsto \mu(g) = g \mapsto [-\mu(g)] + \mu(g) = g \mapsto 0 \\
g \mapsto \mu(g) + g \mapsto -\mu(g) = g \mapsto \mu(g) + [-\mu(g)] = g \mapsto 0
\end{aligned}$$

(5) For all $g \mapsto \mu(g), g \mapsto \nu(g), g \mapsto \sigma(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
[g \mapsto \mu(g) * g \mapsto \nu(g)] * g \mapsto \sigma(g) &= g \mapsto \mu\nu(g) * g \mapsto \sigma(g) \\
&= g \mapsto \mu\nu\sigma(g) \\
&= g \mapsto \mu(g) * g \mapsto \nu\sigma(g) \\
&= g \mapsto \mu(g) * [g \mapsto \nu(g) * g \mapsto \sigma(g)]
\end{aligned}$$

(6) For some unity element $g \mapsto g \in \mathrm{Mor}(G, G)$, for all $g \mapsto \mu(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
g \mapsto g * g \mapsto \mu(g) = g \mapsto \mu(g) \\
g \mapsto \mu(g) * g \mapsto g = g \mapsto \mu(g)
\end{aligned}$$

(7) For all $g \mapsto \lambda(g), g \mapsto \mu(g), g \mapsto \nu(g) \in \mathrm{Mor}(G, G)$:

$$\begin{aligned}
g \mapsto \lambda(g) * [g \mapsto \mu(g) + g \mapsto \nu(g)] &= g \mapsto \lambda(g) * g \mapsto \mu(g) + \nu(g) \\
&= g \mapsto \lambda\mu(g) + \lambda\nu(g) \\
&= g \mapsto \lambda\mu(g) + g \mapsto \lambda\nu(g) \\
&= [g \mapsto \lambda(g) * g \mapsto \mu(g)] + [g \mapsto \lambda(g) * g \mapsto \nu(g)] \\
[g \mapsto \mu(g) + g \mapsto \nu(g)] * g \mapsto \lambda(g) &= g \mapsto \mu(g) + \nu(g) * g \mapsto \lambda(g) \\
&= g \mapsto \mu\lambda(g) + \nu\lambda(g) \\
&= g \mapsto \mu\lambda(g) + g \mapsto \nu\lambda(g) \\
&= [g \mapsto \mu(g) * g \mapsto \lambda(g)] + [g \mapsto \nu(g) * g \mapsto \lambda(g)]
\end{aligned}$$

Hence, $\mathrm{Mor}(G, G)$ is a ring with unity.

Part 3: We prove that c_σ is a ring isomorphism.
(1) As c_σ has an inverse $c_{\sigma^{-1}} : \text{Mor}(G', G') \to \text{Mor}(G, G), \tau' \mapsto \sigma^{-1}\tau'\sigma$, c_σ is bijective.
(2) For all $\tau, \omega \in \text{Mor}(G, G)$:

$$\begin{aligned} c_\sigma(\tau + \omega) &= \sigma(\tau + \omega)\sigma^{-1} \\ &= \sigma\tau\sigma^{-1} + \sigma\omega\sigma^{-1} \\ &= c_\sigma(\tau) + c_\sigma(\omega) \end{aligned}$$

(3) For all $\tau, \omega \in \text{Mor}(G, G)$:

$$\begin{aligned} c_\sigma(\tau\omega) &= \sigma\tau\omega\sigma^{-1} \\ &= \sigma\tau\sigma^{-1}\sigma\omega\sigma^{-1} \\ &= c_\sigma(\tau)c_\sigma(\omega) \end{aligned}$$

(4) For the unity element $e_G \in \text{Mor}(G, G)$:

$$\begin{aligned} c_\sigma(e_G) &= \sigma e_G \sigma^{-1} \\ &= e_{G'} \end{aligned}$$

Hence, c_σ is a ring isomorphism.
Quod. Erat. Demonstrandum. □

Example 3.2. Let $\mathbb{Z}^\mathbb{N}$ be the set of all integral-valued sequences,
which forms an Abelian group under addition.
The following three functions are ring homomorphisms in $\text{Mor}(\mathbb{Z}^\mathbb{N}, \mathbb{Z}^\mathbb{N})$:

$$\begin{aligned} \text{Left} &: (a_1, a_2, a_3, \cdots) \mapsto (a_2, a_3, a_4, \cdots) \\ \text{Right} &: (a_1, a_2, a_3, \cdots) \mapsto (0, a_1, a_2, \cdots) \\ \text{Lead} &: (a_1, a_2, a_3, \cdots) \mapsto (a_1, 0, 0, \cdots) \end{aligned}$$

(1) As Left is not injective, Left has no left inverse.
(2) As $\forall n \in \mathbb{Z}, \text{Left}(n\text{Lead}+\text{Right}) = e_{\mathbb{Z}^\mathbb{N}}$, Left has infinitely many right inverses.

3.2 Quaternion Ring

Proposition 3.3. Let $\mathbf{H}(\mathbb{R})$ be the set of all 2 by 2 matrices in the form:

$$\begin{pmatrix} +w + x\text{i} & -y - z\text{i} \\ +y - z\text{i} & +w - x\text{i} \end{pmatrix}$$

$\mathbf{H}(\mathbb{R})$ is a subring of $\mathbf{M}_2(\mathbb{C})$, where any nonzero element is a unit.

Proof. We may divide our proof into two parts.

Part 1: We prove that $\mathbf{H}(\mathbb{R})$ is a subring of $\mathbf{M}_2(\mathbb{C})$.

(1) For all $\begin{pmatrix} +w+x\mathrm{i} & -y-z\mathrm{i} \\ +y-z\mathrm{i} & +w-x\mathrm{i} \end{pmatrix}, \begin{pmatrix} +w'+x'\mathrm{i} & -y'-z'\mathrm{i} \\ +y'-z'\mathrm{i} & +w'-x'\mathrm{i} \end{pmatrix} \in \mathbf{H}(\mathbb{R})$,
their sum is of the following form:

$$\begin{pmatrix} +(w+w')+(x+x')\mathrm{i} & -(y+y')-(z+z')\mathrm{i} \\ +(y+y')-(z+z')\mathrm{i} & +(w+w')-(x+x')\mathrm{i} \end{pmatrix}$$

Hence, $\mathbf{H}(\mathbb{R})$ is closed under addition.

(2) For all $\begin{pmatrix} +w+x\mathrm{i} & -y-z\mathrm{i} \\ +y-z\mathrm{i} & +w-x\mathrm{i} \end{pmatrix} \in \mathbf{H}(\mathbb{R})$,
its negative element is of the following form:

$$\begin{pmatrix} -w-x\mathrm{i} & +y+z\mathrm{i} \\ -y+z\mathrm{i} & -w+x\mathrm{i} \end{pmatrix}$$

Hence, $\mathbf{H}(\mathbb{R})$ is closed under negative element.

(3) The zero matrix is of the following form:

$$\begin{pmatrix} +0+0\mathrm{i} & -0-0\mathrm{i} \\ +0-0\mathrm{i} & +0-0\mathrm{i} \end{pmatrix}$$

Hence, $\mathbf{H}(\mathbb{R})$ contains the zero element.

(4) For all $\begin{pmatrix} +w+x\mathrm{i} & -y-z\mathrm{i} \\ +y-z\mathrm{i} & +w-x\mathrm{i} \end{pmatrix}, \begin{pmatrix} +w'+x'\mathrm{i} & -y'-z'\mathrm{i} \\ +y'-z'\mathrm{i} & +w'-x'\mathrm{i} \end{pmatrix} \in \mathbf{H}(\mathbb{R})$,
their product is of the following form:

$$\begin{pmatrix} +(ww'-xx'-yy'-zz') & -(wy'-xz'+yw'+zx') \\ +(wx'+xw'+yz'-zy')\mathrm{i} & -(wz'+xy'-yx'+zw')\mathrm{i} \\ +(wy'-xz'+yw'+zx') & +(ww'-xx'-yy'-zz') \\ -(wz'+wy'-yx'+zw')\mathrm{i} & -(wx'+xw'+yz'-zy')\mathrm{i} \end{pmatrix}$$

Hence, $\mathbf{H}(\mathbb{R})$ is closed under multiplication.

(5) The identity matrix is of the following form:

$$\begin{pmatrix} +1+0\mathrm{i} & -0-0\mathrm{i} \\ +0-0\mathrm{i} & +1-0\mathrm{i} \end{pmatrix}$$

Hence, $\mathbf{H}(\mathbb{R})$ contains the unity element.

To conclude, $\mathbf{H}(\mathbb{R})$ is a subring of $\mathbf{M}_2(\mathbb{C})$.

Part 2: We prove that every nonzero element of $\mathbf{H}(\mathbb{R})$ is a unit.

For all nonzero $\begin{pmatrix} +w+x\mathrm{i} & -y-z\mathrm{i} \\ +y-z\mathrm{i} & +w-x\mathrm{i} \end{pmatrix} \in \mathbf{H}(\mathbb{R})$, it has the following reciprocal in $\mathbf{H}(\mathbb{R})$:

$$\frac{1}{w^2+x^2+y^2+z^2} \begin{pmatrix} +w-x\mathrm{i} & +y+z\mathrm{i} \\ -y+z\mathrm{i} & +w+x\mathrm{i} \end{pmatrix}$$

Hence, $\begin{pmatrix} +w + x\mathrm{i} & -y - z\mathrm{i} \\ +y - z\mathrm{i} & +w - x\mathrm{i} \end{pmatrix}$ is a unit.

Quod. Erat. Demonstrandum. □

Remark: *If we apply the following two identifications:*

$$\begin{pmatrix} +w + 0\mathrm{i} & -0 - 0\mathrm{i} \\ +0 - 0\mathrm{i} & +w - 0\mathrm{i} \end{pmatrix} = w \in \mathbb{R}$$

$$\begin{pmatrix} +0 + x\mathrm{i} & -y - z\mathrm{i} \\ +y - z\mathrm{i} & +0 - x\mathrm{i} \end{pmatrix} = x\mathbf{i} + y\mathbf{j} + z\mathbf{k} \in \mathbb{R}^3$$

Then we have the following compact multiplication formula:

$$(w + \mathbf{x})(w' + \mathbf{x}') = ww' - \mathbf{x} \cdot \mathbf{x}' + w\mathbf{x}' + w'\mathbf{x} + \mathbf{x} \times \mathbf{x}'$$

It is the noncommutative part $\mathbf{x} \times \mathbf{x}'$ *that gives the following important application.*

Proposition 3.4. On the real inner product space $\mathbf{H}(\mathbb{R})$, define:

$$\mathrm{e}^{\mathbf{q}} = \frac{1}{0!} + \frac{\mathbf{q}}{1!} + \frac{\mathbf{q}^2}{2!} + \frac{\mathbf{q}^3}{3!} + \cdots$$

For all scalar $\theta \in \mathbb{R}$ and vectors $\mathbf{n}, \mathbf{x} \in \mathbb{R}^3$ with $\|\mathbf{n}\| = 1$:

$$\mathrm{e}^{+\theta\mathbf{n}/2}\mathbf{x}\mathrm{e}^{-\theta\mathbf{n}/2} = (\mathbf{n} \cdot \mathbf{x})\mathbf{n} + \cos\theta[\mathbf{x} - (\mathbf{n} \cdot \mathbf{x})\mathbf{n}] + \sin\theta\mathbf{n} \times \mathbf{x}$$

Proof. Write $\mathbb{R}^3$ as a direct sum of $\langle \mathbf{n} \rangle$ and $\langle \mathbf{n} \rangle^\perp$.

Part 1: If $\mathbf{x} \in \langle \mathbf{n} \rangle$, then $(\mathbf{n} \cdot \mathbf{x})\mathbf{n} = \mathbf{x}$ and $\mathbf{n} \times \mathbf{x} = \mathbf{0}$.

$$\begin{aligned}
\text{[Left Hand Side]} &= \left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\mathbf{n}\right)\mathbf{x}\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \left(0 - \sin\frac{\theta}{2}\mathbf{n} \cdot \mathbf{x} + \cos\frac{\theta}{2}\mathbf{x} + \mathbf{0} + \mathbf{0}\right)\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \left(-\sin\frac{\theta}{2}\mathbf{n} \cdot \mathbf{x} + \cos\frac{\theta}{2}\mathbf{x}\right)\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \left(-\sin\frac{\theta}{2}\mathbf{n} \cdot \mathbf{x}\right)\cos\frac{\theta}{2} - \left(\cos\frac{\theta}{2}\mathbf{x}\right) \cdot \left(-\sin\frac{\theta}{2}\mathbf{n}\right) \\
&+ \left(-\sin\frac{\theta}{2}\mathbf{n} \cdot \mathbf{x}\right)\left(-\sin\frac{\theta}{2}\mathbf{n}\right) + \cos\frac{\theta}{2}\left(\cos\frac{\theta}{2}\mathbf{x}\right) \\
&+ \left(-\sin\frac{\theta}{2}\mathbf{n}\right) \times \left(\cos\frac{\theta}{2}\mathbf{x}\right) = \mathbf{x} = \text{[Right Hand Side]}
\end{aligned}$$

Part 2: If $\mathbf{x} \in \langle \mathbf{n} \rangle^{\perp}$, then $\mathbf{n} \cdot \mathbf{x} = 0$.

$$\begin{aligned}
\text{[Left Hand Side]} &= \left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\mathbf{n}\right)\mathbf{x}\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \left(0 - 0 + \cos\frac{\theta}{2}\mathbf{x} + \mathbf{0} + \sin\frac{\theta}{2}\mathbf{n} \times \mathbf{x}\right)\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \left(\cos\frac{\theta}{2}\mathbf{x} + \sin\frac{\theta}{2}\mathbf{n} \times \mathbf{x}\right)\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\mathbf{n}\right) \\
&= 0 - 0 + \cos\frac{\theta}{2}\left(\cos\frac{\theta}{2}\mathbf{x} + \sin\frac{\theta}{2}\mathbf{n} \times \mathbf{x}\right) \\
&\quad + \mathbf{0} + \left(\cos\frac{\theta}{2}\mathbf{x} + \sin\frac{\theta}{2}\mathbf{n} \times \mathbf{x}\right) \times \left(-\sin\frac{\theta}{2}\mathbf{n}\right) \\
&= \cos\theta\mathbf{x} + \sin\theta\mathbf{n} \times \mathbf{x} = \text{[Right Hand Side]}
\end{aligned}$$

Part 3: In general, $\mathbf{x} = (\mathbf{n} \cdot \mathbf{x})\mathbf{n} + \mathbf{x} - (\mathbf{n} \cdot \mathbf{x})\mathbf{n}$,
where $(\mathbf{n} \cdot \mathbf{x})\mathbf{n} \in \langle \mathbf{n} \rangle$ and $\mathbf{x} - (\mathbf{n} \cdot \mathbf{x})\mathbf{n} \in \langle \mathbf{n} \rangle^{\perp}$,
and we've shown that the two linear mappings are equal.
Quod. Erat. Demonstrandum. □

4 Commutative Ring

4.1 Prime Ideal and Coprime Ideals

*If the multiplication $*$ is commutative, then we can do modular arithmetic,
and there is no need to emphasize that each ideal is two-sided.*

Definition 4.1. (**Prime Element**)
Let R be a commutative ring with unity, and p be a nonunit element of R.
If $p \neq 0$ and $\forall p \nmid a, \forall p \nmid b, p \nmid ab$, then p is prime.

Definition 4.2. (**Prime Ideal**)
Let R be a commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of R.
If $\forall \mathfrak{p} \not\supseteq \mathfrak{a}, \forall \mathfrak{p} \not\supseteq \mathfrak{b}, \mathfrak{p} \not\supseteq \mathfrak{ab}$, then $\mathfrak{p}$ is prime.

Remark: *Note that 0 is not prime but $\{0\}$ is prime.*

Example 4.3. Let R be a commutative ring with unity. As $p \nmid a$ iff $\langle p \rangle \not\ni a$, a nonzero principal ideal $\mathfrak{p}$ is prime iff it is generated by a prime element p.

Remark: *Prime ideal is a generalization of prime element.*

Proposition 4.4. Let R be a commutative ring with unity, and $\mathfrak{p}$ be an ideal of R. $\mathfrak{p}$ is prime iff $\mathfrak{p}^c$ is nonempty and closed under multiplication.

Proof. We may divide our proof into two parts.
"if" direction: Assume that $\mathfrak{p}^c$ is nonempty and closed under multiplication.
(1) As $\mathfrak{p}^c$ is nonempty, $\mathfrak{p}$ is not R.
(2) For all ideals $\mathfrak{a}, \mathfrak{b}$ of R:

$$\begin{aligned}\mathfrak{p} \not\supseteq \mathfrak{a} \text{ and } \mathfrak{p} \not\supseteq \mathfrak{b} &\implies \exists a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}, \mathfrak{p}^c \ni a, b \\ &\implies \exists ab \in \mathfrak{ab}, \mathfrak{p}^c \ni ab \\ &\implies \mathfrak{p} \not\supseteq \mathfrak{ab}\end{aligned}$$

Hence, $\mathfrak{p}$ is prime.
"only if" direction: Assume that $\mathfrak{p}$ is prime.
(1) As $\mathfrak{p}$ is not R, $\mathfrak{p}^c$ is nonempty.
(2) For all elements a, b of R:

$$\begin{aligned}\mathfrak{p}^c \ni a \text{ and } \mathfrak{p}^c \ni b &\implies \mathfrak{p} \not\supseteq \mathfrak{a} = \langle a \rangle \text{ and } \mathfrak{p} \not\supseteq \mathfrak{b} = \langle b \rangle \\ &\implies \mathfrak{p} \not\supseteq \mathfrak{ab} = \langle a \rangle \langle b \rangle \\ &\implies \mathfrak{p}^c \ni ab\end{aligned}$$

Hence, $\mathfrak{p}^c$ is nonempty and closed under multiplication.
Combine the two parts above, we've proven the biconditional.
Quod. Erat. Demonstrandum. □

Proposition 4.5. Let R be a commutative ring with unity,
and I be an ideal of R. I is prime iff R/I is an integral domain.

Proof.

$$\begin{aligned}\mathfrak{p} \text{ is prime} &\iff \mathfrak{p} \neq R \text{ and } \forall a, b \in \mathfrak{p}^c, ab \in \mathfrak{p}^c \\ &\iff R/\mathfrak{p} \neq \{\mathfrak{p}\} \text{ and } \forall a + \mathfrak{p}, b + \mathfrak{p} \neq \mathfrak{p}, (a + \mathfrak{p})(b + \mathfrak{p}) \neq \mathfrak{p} \\ &\iff R/\mathfrak{p} \text{ is an integral domain}\end{aligned}$$

Quod. Erat. Demostrandum. □

Proposition 4.6. Let R, R' be two commutative rings with unity,
and $\sigma : R \to R'$ be a ring homomorphism.
(1) If $\mathfrak{p} \supseteq \operatorname{Ker}(\sigma)$ is a prime ideal of R and σ is surjective,
then $\sigma(\mathfrak{p})$ is a prime ideal of R.
(2) If $\mathfrak{p}'$ is a prime ideal of R',
then $\sigma^{-1}(\mathfrak{p}')$ is a prime ideal of R.

Proof. We may divide our proof into two parts.
Part 1: We prove that the ideal $\sigma(\mathfrak{p})$ of R' is prime.

(1) For all $r \in R$:

$$\begin{aligned} r \in \sigma^{-1}(\sigma(\mathfrak{p})) &\implies \sigma(r) \in \sigma(\mathfrak{p}) \\ &\implies \exists s \in \mathfrak{p}, \sigma(r) = \sigma(s) \\ &\implies \sigma(r-s) = 0' \\ &\implies r-s \in \operatorname{Ker}(\sigma) \subseteq \mathfrak{p} \\ &\implies r = s + (r-s) \in \mathfrak{p} \end{aligned}$$

Hence, $\sigma^{-1}(\sigma(\mathfrak{p})) = \mathfrak{p}$, $\mathfrak{p}$ is saturated.
(2) Assume to the contrary that $\sigma(\mathfrak{p})$ is R, now $\mathfrak{p} = \sigma^{-1}(R')$ is R, contradiction. Hence, our assumption is false, and $\mathfrak{p}$ is not R.
(3) For all ideals $\mathfrak{a}', \mathfrak{b}'$ of R':

$$\begin{aligned} \sigma(\mathfrak{p}) \supseteq \mathfrak{a}'\mathfrak{b}' &\implies \mathfrak{p} = \sigma^{-1}(\sigma(\mathfrak{p})) \supseteq \sigma^{-1}(\mathfrak{a}'\mathfrak{b}') \supseteq \sigma^{-1}(\mathfrak{a}')\sigma^{-1}(\mathfrak{b}') \\ &\implies \mathfrak{p} \supseteq \sigma^{-1}(\mathfrak{a}') \text{ or } \mathfrak{p} \supseteq \sigma^{-1}(\mathfrak{b}') \\ &\implies \sigma(\mathfrak{p}) \supseteq \sigma(\sigma^{-1}(\mathfrak{a}')) = \mathfrak{a}' \text{ or } \sigma(\mathfrak{p}) \supseteq \sigma(\sigma^{-1}(\mathfrak{b}')) = \mathfrak{b}' \end{aligned}$$

To conclude, $\sigma(\mathfrak{p})$ is prime ideal of R'.
Part 2: We prove that the ideal $\sigma^{-1}(\mathfrak{p}')$ of R is prime.
(1) Assume to the contrary that $1 \in \sigma^{-1}(\mathfrak{p}')$, then $1' = \sigma(1) \in \mathfrak{p}'$, contradicting to $\mathfrak{p}' \not\ni 1'$. Hence, our assumption is false, and $\sigma^{-1}(\mathfrak{p}') \not\ni 1$ is not R.
(2) For all ideals $\mathfrak{a}, \mathfrak{b}$ of R:

$$\begin{aligned} \sigma^{-1}(\mathfrak{p}) \supseteq \mathfrak{a}\mathfrak{b} &\implies \mathfrak{p} \supseteq \sigma(\sigma^{-1}(\mathfrak{p})) \supseteq \sigma(\mathfrak{a}\mathfrak{b}) = \sigma(\mathfrak{a})\sigma(\mathfrak{b}) \\ &\implies \mathfrak{p} \supseteq \sigma(\mathfrak{a}) \text{ or } \mathfrak{p} \supseteq \sigma(\mathfrak{b}) \\ &\implies \sigma^{-1}(\mathfrak{p}) \supseteq \mathfrak{a} \text{ or } \sigma^{-1}(\mathfrak{p}) \supseteq \mathfrak{b} \end{aligned}$$

To conclude, $\sigma^{-1}(\mathfrak{p}')$ is a prime ideal of R.
Quod. Erat. Demonstrandum. □

Remark: *The assumption $\mathfrak{p} \supseteq \operatorname{Ker}(\sigma)$ is necessary. Consider the example $R = \mathbb{Z}, R' = \mathbb{Z}_2, \sigma : n \mapsto [n]_2, \mathfrak{p} = 3\mathbb{Z}$. $\mathfrak{p}$ is prime in $\mathbb{Z}$, but $\sigma(\mathfrak{p}) = \mathbb{Z}_2$ is not prime in $\mathbb{Z}_2$.*

Definition 4.7. (**Spectrum**)
Let R be a commutative ring with unity.
Define $\operatorname{Spec}(R) = [\text{All prime ideals of } R]$ as the spectrum of R.

Definition 4.8. (**Vanishing Set**)
Let R be a commutative ring with unity, and $\mathfrak{a}$ be an ideal of R.
Define $Z(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(R) : \mathfrak{p} \supseteq \mathfrak{a}\}$ as the vanishing set at $\mathfrak{a}$.

Lemma 4.9. Let R be a commutative ring with unity, $(\mathfrak{a}_\lambda)_{\lambda\in\Lambda}$ be an indexed family of ideals of R, and $\mathfrak{a} = \sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$ be the sum of $(\mathfrak{a}_\lambda)_{\lambda\in\Lambda}$.

$$\bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda) = Z(\mathfrak{a})$$

Proof. We may divide our proof into two parts.
"$\subseteq$" inclusion: For all $\mathfrak{p} \in \bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda)$, we want to show $\mathfrak{p}$ contains $\mathfrak{a}$.
For all $r \in \mathfrak{a}$, for some finite subset U of Λ and some $(r_\mu)_{\mu\in U}$ in $(\mathfrak{a}_\mu)_{\mu\in U}$, $r = \sum_{\mu\in U} r_\mu$.
As $\mathfrak{p}$ contains each $\mathfrak{a}_\mu$, $\mathfrak{p}$ must contain each r_μ, which implies $r = \sum_{\mu\in U} r_\mu \in \mathfrak{p}$.
Hence, $\mathfrak{p}$ contains $\mathfrak{a}$, which implies $\bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda) \subseteq Z(\mathfrak{a})$.
"$\supseteq$" inclusion: For all $\mathfrak{p} \in Z(\mathfrak{a})$, we want to show $\mathfrak{p}$ contains each $\mathfrak{a}_\lambda$.
As $\mathfrak{a}_\lambda$ is a subset of $\mathfrak{a}$ and $\mathfrak{p}$ contains $\mathfrak{a}$, $\mathfrak{p}$ contains $\mathfrak{a}_\lambda$, which implies $\bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda) \supseteq Z(\mathfrak{a})$.
Hence, $\bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda) = Z(\mathfrak{a})$. Quod. Erat. Demonstrandum. □

Lemma 4.10. Let R be a commutative ring with unity, $(\mathfrak{a}_k)_{k=1}^m$ be a finite list of ideals of R, and $\mathfrak{a} = \prod_{k=1}^m \mathfrak{a}_k$ be the product of $(\mathfrak{a}_k)_{k=1}^m$.

$$\bigcup_{k=1}^m Z(\mathfrak{a}_k) = Z(\mathfrak{a})$$

Proof. We may divide our proof into two parts.
"$\subseteq$" inclusion: For all $1 \leq k \leq m$ and $\mathfrak{p} \in Z(\mathfrak{a}_k)$, we want to show $\mathfrak{p}$ contains $\mathfrak{a}$.
As $\mathfrak{a}$ is a subset of $\mathfrak{a}_k$ and $\mathfrak{p}$ contains $\mathfrak{a}_k$, $\mathfrak{p}$ contains $\mathfrak{a}$, which implies $\bigcup_{k=1}^m Z(\mathfrak{a}_k) \subseteq Z(\mathfrak{a})$.
"$\supseteq$" inclusion: For all $\mathfrak{p} \in Z(\mathfrak{a})$, we want to show $\mathfrak{p}$ contains some $\mathfrak{a}_k$.
As $\mathfrak{p}$ is prime, $\mathfrak{p}$ contains $\mathfrak{a}$ implies $\mathfrak{p}$ contains some $\mathfrak{a}_k$, which implies $\bigcup_{k=1}^m Z(\mathfrak{a}_k) \supseteq Z(\mathfrak{a})$.
Hence, $\bigcup_{k=1}^m Z(\mathfrak{a}_k) = Z(\mathfrak{a})$. Quod. Erat. Demonstrandum. □

Proposition 4.11. Let R be a nonzero commutative ring with unity.
$\mathcal{C}_{\mathrm{Spec}(R)} = \{Z(\mathfrak{a}) \subseteq \mathrm{Spec}(R) : \mathfrak{a} \text{ is an ideal of } R\}$ is a topology on $\mathrm{Spec}(R)$.

Proof. We may divide our proof into three parts.
Part 1: $\emptyset = Z(R) \in \mathcal{C}_{\mathrm{Spec}(R)}$ and $\mathrm{Spec}(R) = Z(\{0\}) \in \mathcal{C}_{\mathrm{Spec}(R)}$.
Part 2: For all indexed family $(Z(\mathfrak{a}_\lambda))_{\lambda\in\Lambda}$ in $\mathcal{C}_{\mathrm{Spec}(R)}$:

$$\bigcap_{\lambda\in\Lambda} Z(\mathfrak{a}_\lambda) = Z\left(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda\right) \in \mathrm{Spec}(R)$$

Part 3: For all finite list $(Z(\mathfrak{a}_k))_{k=1}^m$ in $\mathcal{C}_{\mathrm{Spec}(R)}$:

$$\bigcup_{k=1}^m Z(\mathfrak{a}_k) = Z\left(\prod_{k=1}^m \mathfrak{a}_k\right) \in \mathrm{Spec}(R)$$

Combine the three parts above, we've proven that $\mathcal{C}_{\mathrm{Spec}(R)}$ is a topology on $\mathrm{Spec}(R)$. Quod. Erat. Demonstrandum. □

Proposition 4.12. Define the followings:
(1) $\mathrm{Obj} =$ [All nonzero commutative rings with unity].
(2) $\mathrm{Mor} =$ [All ring homomorphisms].
(3) $\mathrm{Obj}' =$ [All nonempty topological spaces].
(4) $\mathrm{Mor}' =$ [All continuous functions].
$\mathrm{Spec} : R \mapsto \mathrm{Spec}(R), (r \mapsto \sigma(r)) \mapsto (\mathfrak{p}_S \mapsto \sigma^{-1}(\mathfrak{p}_S))$ is a contravariant functor.

Proof. We may divide our proof into three parts.
Part 1: We prove that Spec is well-defined.
For all $R, S \in \mathrm{Obj}$, for all $\sigma \in \mathrm{Mor}(R, S)$,
we wish to show $\sigma' = \mathrm{Spec}(\sigma) \in \mathrm{Mor}'(\mathrm{Spec}(S), \mathrm{Spec}(R))$.
That is, for all $U = Z(\mathfrak{a}_R) \in \mathcal{C}_{\mathrm{Spec}(R)}$, we wish to show $\sigma'^{-1}(U) \in \mathcal{C}_{\mathrm{Spec}(S)}$.

$$\begin{aligned} \sigma'^{-1}(U) &= \{\mathfrak{p}_S \in \mathrm{Spec}(S) : \sigma'(\mathfrak{p}_S) \in U\} \\ &= \{\mathfrak{p}_S \in \mathrm{Spec}(S) : \sigma^{-1}(\mathfrak{p}_S) \in Z(\mathfrak{a}_R)\} \\ &= \{\mathfrak{p}_S \in \mathrm{Spec}(S) : \sigma^{-1}(\mathfrak{p}_S) \supseteq \mathfrak{a}_R\} \\ &= \{\mathfrak{p}_S \in \mathrm{Spec}(S) : \mathfrak{p}_S \supseteq \sigma(\mathfrak{a}_R)\} \\ &= Z(\sigma(\mathfrak{a}_R)) \in \mathrm{Spec}(S) \end{aligned}$$

Hence, σ' is continuous, Spec is well-defined.
Part 2: We prove that Spec preserves the identity function.
For all $R \in \mathrm{Obj}$:

$$\mathrm{Spec}(r \mapsto r) = \mathfrak{p}_R \mapsto \mathfrak{p}_R$$

Part 3: We prove that Spec reverses composition.
For all $R, S, T \in \mathrm{Obj}$, for all $\sigma \in \mathrm{Mor}(R, S)$ and $\tau \in \mathrm{Mor}(S, T)$:

$$\begin{aligned} \mathrm{Spec}(s \mapsto \tau(s) * r \mapsto \sigma(r)) &= \mathrm{Spec}(r \mapsto \tau\sigma(r)) \\ &= \mathfrak{p}_T \mapsto \sigma^{-1}\tau^{-1}(\mathfrak{p}_T) \\ &= \mathfrak{p}_S \mapsto \sigma^{-1}(\mathfrak{p}_S) * \mathfrak{p}_T \mapsto \tau^{-1}(\mathfrak{p}_T) \\ &= \mathrm{Spec}(r \mapsto \sigma(r)) * \mathrm{Spec}(s \mapsto \tau(s)) \end{aligned}$$

To conclude, Spec is a contravariant functor. Quod. Erat. Demonstrandum. □

Definition 4.13. (**Coprime Ideals**)
Let R be a commutative ring with unity, and $\mathfrak{a}, \mathfrak{b}$ be two ideals of R.
If $\mathfrak{a} + \mathfrak{b} = R$, then $\mathfrak{a}, \mathfrak{b}$ are coprime.

Lemma 4.14. Let R be a commutative ring with unity, and I be an ideal of R. For all $a \in R$, $\langle a \rangle, I$ are coprime in R iff $a + I$ is a unit in R/I.

Proof.

$$\begin{aligned}
\langle a \rangle, I \text{ are coprime in } R &\iff \langle a \rangle + I = R \\
&\iff \exists x \in R \text{ and } r \in I, xa + r = 1 \\
&\iff \exists x + I \in R/I, (x + I)(a + I) = 1 + I \\
&\iff a + I \text{ is a unit in } R/I
\end{aligned}$$

Quod. Erat. Demonstrandum. □

Lemma 4.15. Let R be a commutative ring with unity, and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m (m \geq 2)$ be a finite list of pairwisely coprime ideals of R.

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_m = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_m$$

Proof. We prove this lemma by mathematical induction.
Basis Step: When $m = 2$:
(1) For all $r \in \mathfrak{p}_1 \mathfrak{p}_2$, WLOG, assume that for some $r_1 \in \mathfrak{p}_1$ and $r_2 \in \mathfrak{p}_2$, $r = r_1 r_2$.

$$\left.\begin{array}{rcrcr}
r_1 \in \mathfrak{p}_1 & \text{and} & r_2 \in R & \implies & r = r_1 r_2 \in \mathfrak{p}_1 \\
r_1 \in R & \text{and} & r_2 \in \mathfrak{p}_2 & \implies & r = r_1 r_2 \in \mathfrak{p}_2
\end{array}\right\} \implies r \in \mathfrak{p}_1 \cap \mathfrak{p}_2$$

(2) For all $r \in \mathfrak{p}_1 \cap \mathfrak{p}_2$, choose $r_1 \in \mathfrak{p}_1$ and $r_2 \in \mathfrak{p}_2$, such that $1 = r_1 + r_2 \in \mathfrak{p}_1 + \mathfrak{p}_2$.

$$\left.\begin{array}{rcrcr}
r_1 \in \mathfrak{p}_1 & \text{and} & r \in \mathfrak{p}_2 & \implies & r_1 r \in \mathfrak{p}_1 \mathfrak{p}_2 \\
r \in \mathfrak{p}_1 & \text{and} & r_2 \in \mathfrak{p}_2 & \implies & r r_2 \in \mathfrak{p}_1 \mathfrak{p}_2
\end{array}\right\} \implies r = r_1 r + r r_2 \in \mathfrak{p}_1 \mathfrak{p}_2$$

Hence, $\mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1 \mathfrak{p}_2$, the lemma holds.
Inductive Hypothesis: For all $l \geq 2$, when $m = l$, assume that the lemma holds.
Inductive Step: When $m = l + 1$:

$$\begin{aligned}
\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_l \cap \mathfrak{p}_{l+1} &= (\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_l) \cap \mathfrak{p}_{l+1} \\
&= (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_l) \cap \mathfrak{p}_{l+1} \\
&= (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_l) \mathfrak{p}_{l+1} \\
&= \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_l \mathfrak{p}_{l+1}
\end{aligned}$$

Hence, the lemma is true for all $m \geq 2$. Quod. Erat. Demonstrandum. □

Lemma 4.16. Let R be a commutative ring with unity, and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m (m \geq 2)$ be a finite list of pairwisely coprime ideals of R.

$$(1+\mathfrak{p}_1) \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_m \neq \emptyset$$

Proof. We may divide our proof into three steps.
Step 1: As $\mathfrak{p}_2, \cdots, \mathfrak{p}_m$ are pairwisely coprime, it suffices to prove the following:

$$(1+\mathfrak{p}_1) \cap (\mathfrak{p}_2 \cdots \mathfrak{p}_m) \neq \emptyset$$

Step 2: As $\mathfrak{p}_1$ is coprime with the product $\mathfrak{p}_2 \cdots \mathfrak{p}_m$, for some $r_1 \in \mathfrak{p}_1$ and $\pi_1 \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$:

$$r_1 + \pi_1 = 1$$

Step 3: The above construction suggests the following:

$$\mathfrak{p}_1 + \langle \pi_1 \rangle = R$$

Now $\pi_1 + \mathfrak{p}_1$ has a reciprocal $\tau_1 + \mathfrak{p}_1$ in $R/\mathfrak{p}_1$, which implies:

$$\left.\begin{matrix} (\pi_1+\mathfrak{p}_1)(\tau_1+\mathfrak{p}_1) = 1+\mathfrak{p}_1 & \Longrightarrow & \pi_1\tau_1 \in 1+\mathfrak{p}_1 \\ \pi_1 \in \mathfrak{p}_2 \cdots \mathfrak{p}_m \text{ and } \tau_1 \in R & \Longrightarrow & \pi_1\tau_1 \in \mathfrak{p}_2 \cdots \mathfrak{p}_m \end{matrix}\right\} \Longrightarrow \pi_1\tau_1 \in (1+\mathfrak{p}_1) \cap (\mathfrak{p}_2 \cdots \mathfrak{p}_m)$$

Hence, we've constructed an element $\pi_1\tau_1$ in the intersection, which is nonempty.
Quod. Erat. Demonstrandum. □

Theorem 4.17. (**Chinese Remainder Theorem**)
Let R be a commutative ring with unity, and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m (m \geq 2)$ be a finite list of pairwisely coprime ideals of R. The following mapping is a ring isomorphism:

$$\widetilde{\sigma} : \begin{cases} R/\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m & \to & R/\mathfrak{p}_1 \times R/\mathfrak{p}_2 \times \cdots \times R/\mathfrak{p}_m \\ r + \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m & \mapsto & (r+\mathfrak{p}_1, r+\mathfrak{p}_2, \cdots, r+\mathfrak{p}_m) \end{cases}$$

Proof. Define the following mapping:

$$\sigma : \begin{cases} R & \to & R/\mathfrak{p}_1 \times R/\mathfrak{p}_2 \times \cdots \times R/\mathfrak{p}_m \\ r & \mapsto & (r+\mathfrak{p}_1, r+\mathfrak{p}_2, \cdots, r+\mathfrak{p}_m) \end{cases}$$

We want to prove that σ is a surjective ring homomorphism with $\text{Ker}(\sigma) = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m$.

Step 1: Choose the following finite list from R:

$$\begin{aligned}\pi_1\tau_1 &\in (1+\mathfrak{p}_1)\cap\mathfrak{p}_2\cap\cdots\cap\mathfrak{p}_m\\ \pi_2\tau_2 &\in \mathfrak{p}_1\cap(1+\mathfrak{p}_2)\cap\cdots\cap\mathfrak{p}_m\\ &\vdots\\ \pi_m\tau_m &\in \mathfrak{p}_1\cap\mathfrak{p}_2\cap\cdots\cap(1+\mathfrak{p}_m)\end{aligned}$$

For all $(r_1+\mathfrak{p}_1, r_2+\mathfrak{p}_2,\cdots,r_m+\mathfrak{p}_m)\in R/\mathfrak{p}_1\times R/\mathfrak{p}_2\times\cdots\times R/\mathfrak{p}_m$,
it is the image of some $r_1\pi_1\tau_1+r_2\pi_2\tau_2+\cdots+r_m\pi_m\tau_m\in R$ under σ, so σ is surjective.
Step 2: As σ is a direct product of ring homomorphisms, σ is a ring homomorphism.
Step 3: $\mathrm{Ker}(\sigma)=\mathfrak{p}_1\cap\mathfrak{p}_2\cap\cdots\cap\mathfrak{p}_m=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m$.
According to **Theorem 2.24.**, $\widetilde{\sigma}: R/\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m=R/\mathrm{Ker}(\sigma)\to R/\mathfrak{p}_1\times R/\mathfrak{p}_2\times\cdots\times R/\mathfrak{p}_m, r+\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m\mapsto(r+\mathfrak{p}_1,r+\mathfrak{p}_2,\cdots,r+\mathfrak{p}_m)$ is a ring isomorphism.
Quod. Erat. Demonstrandum. □

4.2 Maximal Ideal and Irreducible Element

Definition 4.18. (**Maximal Ideal**)
Let R be a commutative ring with unity, and $\mathfrak{p}$ be a proper ideal of R.
If $\forall a\in\mathfrak{p}^c$, $\langle a\rangle+\mathfrak{p}=R$, then $\mathfrak{p}$ is maximal.

Proposition 4.19. Let R be a commutative ring with unity,
and I be an ideal of R. I is maximal iff R/I is a field.
As a consequence, every maximal ideal is prime.

Proof.

$$\begin{aligned}\mathfrak{p}\text{ is maximal} &\iff \mathfrak{p}\neq R\text{ and }\forall a\in\mathfrak{p}^c,\langle a\rangle+\mathfrak{p}=R\\ &\iff R/\mathfrak{p}\neq\{\mathfrak{p}\}\text{ and }\forall a+\mathfrak{p}\neq\mathfrak{p},\exists x+\mathfrak{p}\in R/\mathfrak{p},(a+\mathfrak{p})(x+\mathfrak{p})=1+\mathfrak{p}\\ &\iff R/\mathfrak{p}\text{ is a field}\end{aligned}$$

Quod. Erat. Demonstrandum. □

Example 4.20. Let $\mathbb{Z}^{\mathbb{N}}$ be the integral convolution ring.
(1) The ideal $\langle 2\delta_{1,n}\rangle=$ [All sequences with even entry] is prime, because:

$$\left.\begin{aligned}a_i\text{ is odd with minimal }i\\ b_j\text{ is odd with minimal }j\end{aligned}\right\}\implies a_1b_{i+j-1}+\cdots+a_ib_j+\cdots+a_{i+j-1}b_1\text{ is odd}$$

(2) The ideal $\langle 2\delta_{1,n}\rangle=$ [All sequences with even entry] is not maximal, because:

$$\exists\text{ ideal }\langle 2\delta_{1,n},\delta_{2,n}\rangle\text{ of }R, \langle 2\delta_{1,n}\rangle\subsetneq\langle 2\delta_{1,n},\delta_{2,n}\rangle\subsetneq R$$

Definition 4.21. (**Irreducible Element**)
Let R be a commutative ring with unity, and p be a nonunit element of R.
If $p \neq 0$ and $\forall a, b \in (R^\times)^c, p \neq ab$, then p is irreducible.

Proposition 4.22. Let R be an integral domain, and p be a nonunit element of R. p is prime implies p is irreducible.

Proof. Assume that p is prime.
(1) p is nonunit and nonzero.
(2) For all elements a, b of R:

$$\begin{aligned} p = ab &\implies p | ab \\ &\implies p|a \text{ or } p|b \\ &\implies 1 = (a/p)b \text{ or } 1 = a(b/p) \\ &\implies a \text{ or } b \text{ is a unit} \end{aligned}$$

Hence, p is irreducible. Quod. Erat. Demonstrandum. □

Example 4.23. Let $\mathbb{Z}_6$ be the set of all integers modulo 6,
which forms a commutative ring with unity under addition and multiplication.
(1) As $\langle 2 \rangle^c = \{1, 3, 5\}$ is closed under multiplication, $\langle 2 \rangle$ is prime, so 2 is prime.
(2) As $\exists 2, 4 \in (\mathbb{Z}_6^\times)^c, 2 = 2 * 4$, 2 is reducible.

4.3 Principal Ideal Ring

Integral domain is similar to integers in sense that there is no zero divisor.
Principal ideal ring is similar to integers in sense that every ideal has a generator.

Definition 4.24. (**Principal Ideal Ring**)
Let R be a commutative ring with unity.
If every ideal $\mathfrak{a}$ of R has a generator a, then R is a principal ideal ring.

Example 4.25. $\mathbb{Z}$ is an integral domain and a principal ideal ring.

Example 4.26. Every field R is an integral domain and a principal ideal ring.

Example 4.27. Let R, R' be two rings, and $\sigma : R \to R'$ be a surjective ring homomorphism. R is a principal ideal ring implies R' is a principal ideal ring.

Proposition 4.28. For all composite number $n \geq 4$,
$\mathbb{Z}_n$ is a principal ideal ring, but not an integral domain.

Proof. As $pq = n \equiv 0 (\text{mod } n)$, where $p, q \geq 2$, $\mathbb{Z}_n$ is not an integral domain.
As $\mathbb{Z}_n$ is the surjective image of $\mathbb{Z}$ under quotient ring homomorphism, $\mathbb{Z}$ is a principal ideal ring implies $\mathbb{Z}_n$ is a principal ideal ring. Quod. Erat. Demonstrandum. □

Remark: *Integral domain property is independent of principal ideal property.*

Proposition 4.29. Let R be a principal ideal ring, and p be an element of R.
If p is irreducible, then $\mathfrak{p} = \langle p \rangle$ is maximal.

Proof. Assume that p is irreducible.
(1) p is nonunit implies $\mathfrak{p} = \langle p \rangle$ is proper.
(2) For all ideal $\mathfrak{a} = \langle a \rangle$ of the principal ideal ring R:

$$\begin{aligned} \mathfrak{p} = \langle p \rangle \subseteq \mathfrak{a} = \langle a \rangle &\implies \exists x \in R, p = xa \\ &\implies x \text{ or } a \text{ is a unit} \\ &\implies \mathfrak{a} = \mathfrak{p} \text{ or } \mathfrak{a} = R \end{aligned}$$

Hence, $\mathfrak{p} = \langle p \rangle$ is maximal. Quod. Erat. Demonstrandum. □

Remark: *Now we have the following results:*
(1) In a commutative ring with unity, $\mathfrak{p} = \langle p \rangle$ is maximal implies $\mathfrak{p} = \langle p \rangle$ is prime.
(2) In a commutative ring with unity, $\mathfrak{p} = \langle p \rangle$ is nonzero and prime iff p is prime.
(3) In an integral domain, p is prime implies p is irreducible.
(4) In a principal ideal ring, p is irreducible implies $\mathfrak{p} = \langle p \rangle$ is maximal.
If we define principal ideal domain as the conjunction of principal ideal ring and integral domain, then the four lines are equivalent.

4.4 Quadratic Extension of a Field

Theorem 4.30. (**Euler's Theorem**)
Let R be a commutative ring with unity, and I be an ideal of R.
$G = \{\langle a \rangle \subseteq R : \langle a \rangle, I \text{ are coprime}\}$ forms an Abelian group under $\langle a \rangle * \langle b \rangle = \langle ab \rangle$.

Proof. We may divide our proof into five parts.
Part 1: We prove that $*$ is well-defined.
(1) For all principal ideals $\langle a \rangle, \langle b \rangle, \langle a' \rangle, \langle b' \rangle$ of R:

$$\begin{aligned} \langle a \rangle = \langle a' \rangle \text{ and } \langle b \rangle = \langle b' \rangle &\implies \exists r, s \in R^{\times}, a = ra' \text{ and } b = sb' \\ &\implies \exists rs \in R^{\times}, ab = rsa'b' \\ &\implies \langle ab \rangle = \langle a'b' \rangle \end{aligned}$$

Hence, the product is unique.
(2) For all principal ideals $\langle a\rangle, \langle b\rangle$ of R:

$$\begin{aligned}\langle a\rangle, \langle b\rangle \text{ are coprime with } I &\implies a+I, b+I \in (R/I)^\times \\ &\implies ab+I = (a+I)(b+I) \in (R/I)^\times \\ &\implies \langle ab\rangle \text{ is coprime with } I\end{aligned}$$

Hence, $*$ is a closed operation.
To conclude, $*$ is well-defined.
Part 2: For all $\langle a\rangle, \langle b\rangle \in G$:

$$\langle a\rangle * \langle b\rangle = \langle ab\rangle = \langle ba\rangle = \langle b\rangle * \langle a\rangle$$

Hence, $*$ is commutative.
Part 3: For all $\langle a\rangle, \langle b\rangle, \langle c\rangle \in G$:

$$\begin{aligned}(\langle a\rangle * \langle b\rangle) * \langle c\rangle &= \langle ab\rangle * \langle c\rangle = \langle (ab)c\rangle \\ &= \langle a(bc)\rangle = \langle a\rangle * \langle bc\rangle = \langle a\rangle * (\langle b\rangle * \langle c\rangle)\end{aligned}$$

Hence, $*$ is associative.
Part 4: We prove that $*$ has an identity $\langle 1\rangle$.
(1) As $1+I \in (R/I)^\times$, $\langle 1\rangle \in G$.
(2) For all $\langle a\rangle \in G$:

$$\langle 1\rangle * \langle a\rangle = \langle 1a\rangle = \langle a\rangle$$

Hence, $*$ has an identity $\langle 1\rangle$.
Part 5: We prove that $*$ is invertible.
(1) For all $\langle a\rangle \in G$, as $a+I \in (R/I)^\times$, $a+I$ has an inverse $x+I \in (R/I)^\times$, so $\langle x\rangle \in G$.
(2) For this $\langle x\rangle \in G$:

$$1+I = (x+I)(a+I) = xa+I \implies \langle x\rangle * \langle a\rangle = \langle xa\rangle = \langle 1\rangle$$

Hence, $*$ is invertible.
Combine the five parts above, we've proven that G forms an Abelian group under $*$.
Quod. Erat. Demonstrandum. □

Remark: *As a corollary, if the group G constructed is finite, then for all $a \in R$:*

$$\langle a\rangle, I \text{ are coprime} \implies a^{|G|} - 1 \in I$$

Theorem 4.31. (**Fermat's Little Theorem**)
Let R be a commutative ring with unity, and I be a maximal ideal of R.
If the field R/I is finite, then every $a \in R$ satisfies $a^{|R/I|} - a \in I$.

Proof. We may prove by cases.
Case 1: Assume that $a \in I$. As I is an ideal, $a^{|R/I|} - a \in I$.
Case 2: Assume that $a \notin I$, so $a + I \in (R/I)^\times$.
According to **Lagrange Theorem**, $\text{Ord}(a + I)$ divides $|(R/I)^\times| = |R/I| - 1$, so:

$$(a + I)^{|R/I|-1} = 1 + I \implies a^{|R/I|-1} - 1 \in I \implies a^{|R/I|} - a \in I$$

In both cases, the theorem holds. Quod. Erat. Demonstrandum. □

Theorem 4.32. (**Wilson's Theorem**)
Let R be a commutative ring with unity, and I be a maximal ideal of R.
If $|R/I|$ is odd, then the product of all nonzero cosets is $-1 + I$.

Proof. For all coset $x + I$ in the field R/I with odd cardinality:

$$\begin{aligned}(x + I)^2 = 1 + I &\iff (x - 1 + I)(x + 1 + I) = 0 + I \\ &\iff x - 1 + I = 0 + I \text{ or } x + 1 + I = 0 + I \\ &\iff x + I = +1 + I \text{ or } x + I = -1 + I\end{aligned}$$

That is, $+1 + I, -1 + I$ are the only two distinct cosets such that $(x + I)^2 = 1 + I$.
Now partition $(R/I)^\times$ by equivalence classes in the form:

$$[x + I] = \{(x + I)^{+1}, (x + I)^{-1}\}$$

Every nonsingleton equivalence class contributes nothing to the product, so:

$$[\text{The product of all nonzero cosets}] = (+1 + I)(-1 + I) = -1 + I$$

Quod. Erat. Demonstrandum. □

Lemma 4.33. Let R be a commutative ring with unity,
and I be a maximal ideal of R. If $|R/I|$ is odd,
and some nonzero coset $a + I$ has a square root, then $a^{(|R/I|-1)/2} - 1 \in I$.

Proof. Assume that $a + I$ has a square root $x + I$,
then **Fermat's Little Theorem** suggests:

$$a^{(|R/I|-1)/2} - 1 = x^{|R/I|-1} - 1 \in I$$

Quod. Erat. Demonstrandum. □

Lemma 4.34. Let R be a commutative ring with unity,
and I be a maximal ideal of R. If $|R/I|$ is odd,
and some nonzero coset $a + I$ has no square root, then $a^{(|R/I|-1)/2} + 1 \in I$.

Proof. For all coset $x + I$ in the field R/I with odd cardinality:

$$(x + I)^2 = a + I \implies \text{Contradiction}$$

Now partition $(R/I)^\times$ by equivalence classes in the form:

$$[x + I] = \{(x + I)^{+1}, (a + I)(x + I)^{-1}\}$$

Every equivalence class is nonsingleton, and every nonsingleton equivalence class contributes a term $(a + I)$ to the product, so **Wilson's Theorem** suggests:

$$a^{(|R/I|-1)/2} + I = (a + I)^{(|R/I|-1)/2} = [\text{The product of all nonzero cosets}] = -1 + I$$

To conclude, $a^{(|R/I|-1)/2} + 1 \in I$. Quod. Erat. Demonstrandum. □

Definition 4.35. (**Legendre's Symbol**)
Let R be a commutative ring with unity,
a be an element of R, and I be a maximal ideal of R.
If $|R/I|$ is odd, then define the Legendre symbol of a modulo I as:

$$(a/I) = 0, \pm 1 \quad \text{if} \quad a^{(|R/I|-1)/2} \in 0, \pm 1 + I;$$

Lemma 4.36. Let R be a commutative ring with unity,
and I be a maximal ideal of R. If $|R/I|$ is odd,
then $\sigma : (R/I)^\times \to \mathbb{Z}^\times, a + I \mapsto (a/I)$ is a group homomorphism.

Proof. In the Abelian group $(R/I)^\times$, any power map is a group homomorphism.
Especially, the power map $\tau : a + I \mapsto a^{(|R/I|-1)/2} + I$ is a group homomorphism.
Hence, the map σ induced by τ is a group homomorphism.
Quod. Erat. Demonstrandum. □

Lemma 4.37. In the field $\mathbb{Z}_p$, where $p \geq 3$ is prime, if $a \neq 0$,
then there exists $b \in \mathbb{Z}_p$, such that $b^2 - a$ has no square root.

Proof. Assume to the contrary that for all $b \in \mathbb{Z}_p$,
$b^2 - a$ has a square root. Fix an arbitrary $b_0 = b \in \mathbb{Z}_p$.
$b^2 - 0a = b_0^2$ has a square root $b_0 \in \mathbb{Z}_p$.
$b^2 - 1a = b_0^2 - a$ has a square root $b_1 \in \mathbb{Z}_p$.
Repeat this process recursively,
and then $a = b^2 - (b^2 - a)a^{-1}a$ has a square root.
Quod. Erat. Demonstrandum. □

Remark: *For large p, computer scientists do random guess to find b.*

Lemma 4.38. Let R be a field, and w^2 be an element of R with no square root. If we define the followings, then $R[w]$ is a field:

$$\begin{aligned} R[w] &= \{x + yw : x, y \in R\} \\ (x + yw) + (x' + y'w) &= (x + x') + (y + y')w \\ (x + yw)(x' + y'w) &= (xx' + yy'w^2) + (xy' + yx')w \end{aligned}$$

Proof. We may divide our proof into nine parts.
Part 1: For all $x + yw, x' + y'w \in R[w]$:

$$\begin{aligned} (x + yw) + (x' + y'w) &= (x + x') + (y + y')w \\ &= (x' + x) + (y' + y)w \\ &= (x' + y'w) + (x + yw) \end{aligned}$$

Part 2: For all $x + yw, x' + y'w, x'' + y''w \in R[w]$:

$$\begin{aligned} [(x + yw) + (x' + y'w)] + (x'' + y''w) &= [(x + x') + (y + y')w] + (x'' + y''w) \\ &= [(x + x') + x''] + [(y + y') + y'']w \\ &= [x + (x' + x'')] + [y + (y' + y'')]w \\ &= (x + yw) + [(x' + x'') + (y' + y'')w] \\ &= (x + yw) + [(x' + y'w) + (x'' + y''w)] \end{aligned}$$

Part 3: For some zero element $0 + 0w \in R[w]$, for all $x + yw \in R[w]$:

$$\begin{aligned} (0 + 0w) + (x + yw) &= (0 + x) + (0 + y)w \\ &= x + yw \end{aligned}$$

Part 4: For all $x + yw \in R[w]$, for some negative element $-x - yw \in R[w]$:

$$\begin{aligned} (-x - yw) + (x + yw) &= (-x + x) + (-y + y)w \\ &= 0 + 0w \end{aligned}$$

Part 5: For all $x + yw, x' + y'w \in R[w]$:

$$\begin{aligned} (x + yw)(x' + y'w) &= (xx' + yy'w^2) + (xy' + yx')w \\ &= (x'x + y'yw^2) + (x'y + y'x)w \\ &= (x' + y'w)(x + yw) \end{aligned}$$

Part 6: For all $x + yw, x' + y'w, x'' + y''w \in R[w]$:

$$\begin{aligned}
[(x + yw)(x' + y'w)](x'' + y''w) &= [(xx' + yy'w^2) + (xy' + yx')w](x'' + y''w) \\
&= (xx'x'' + xy'y''w^2 + yx'y''w^2 + yy'x''w^2) \\
&+ (yx'x'' + xy'x'' + xx'y'' + yy'y''w^2)w \\
&= (x + yw)[(x'x'' + y'y''w^2) + (x'y'' + y'x'')w] \\
&= (x + yw)[(x' + y'w)(x'' + y''w)]
\end{aligned}$$

Part 7: For some unity element $1 + 0w \in R[w]$, for all $x + yw \in R[w]$:

$$\begin{aligned}
(1 + 0w)(x + yw) &= (1x + 0yw^2) + (1y + 0x)w \\
&= x + yw
\end{aligned}$$

Part 8: For all nonzero $x + yw \in R[w]$, note that w^2 has no square root in R implies $x^2 \neq y^2w^2$, so $x^2 - y^2w^2$ has a reciprocal element $\frac{1}{x^2-y^2w^2} \in R^\times$.
This implies the existence of some $\frac{x-yw}{x^2-y^2w^2} \in R[w]$, such that:

$$\begin{aligned}
\frac{(x - yw)(x + yw)}{x^2 - y^2w^2} &= \frac{(x^2 - y^2w^2) + (xy - yx)w}{x^2 - y^2w^2} \\
&= 1 + 0w
\end{aligned}$$

Part 9: For all $\lambda + \mu w, x + yw, x' + y'w \in R[w]$:

$$\begin{aligned}
(\lambda + \mu w)[(x + yw) + (x' + y'w)] &= (\lambda + \mu w)[(x + x') + (y + y')w] \\
&= [\lambda(x + x') + \mu(y + y')w^2] \\
&+ [\lambda(y + y') + \mu(x + x')]w \\
&= [(\lambda x + \mu yw^2) + (\lambda x' + \mu y'w^2)] \\
&+ [(\lambda y + \mu x) + (\lambda y' + \mu x')]w \\
&= [(\lambda x + \mu yw^2) + (\lambda y + \mu x)w] \\
&+ [(\lambda x' + \mu y'w^2) + (\lambda y' + \mu x')w] \\
&= (\lambda + \mu w)(x + yw) + (\lambda + \mu w)(x' + y'w)
\end{aligned}$$

Hence, $R[w]$ is a field. Quod. Erat. Demonstrandum. □

Lemma 4.39. In the field $\mathbb{Z}_p[w]$, where $p \geq 3$ is prime:
(1) For all $z, w \in \mathbb{Z}_p[w]$:

$$(z+w)^p = z^p + w^p$$

(2) For all nonzero real number $x \in \mathbb{Z}_p[w]$:

$$x^p = +x$$

(3) For all nonzero pure imaginary number: $yw \in \mathbb{Z}_p[w]$:

$$y^p w^p = -yw$$

Proof. We may divide our proof into three parts.
Part 1: For all $0 < k < p$, the binomial coefficient $\begin{pmatrix} p \\ k \end{pmatrix}$ is a multiple of p, so:

$$(z+w)^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} z^{p-k} w^k = z^p + \sum_{k=1}^{p-1} [\text{Some multiple of } p] z^{p-k} w^k + w^p = z^p + w^p$$

Part 2: For the nonzero real number $x \in \mathbb{Z}_p[w]$, $(x^2/p) = +1$, so:

$$x^p = (x^2)^{(p-1)/2} x = \left(\frac{x^2}{p} \right) x = +x$$

Part 3: For the nonzero pure imaginary number $yw \in \mathbb{Z}_p[w]$, $(y^2w^2/p) = -1$, so:

$$y^p w^p = (y^2 w^2)^{(p-1)/2} yw = \left(\frac{y^2 w^2}{p} \right) yw = -yw$$

Quod. Erat. Demonstrandum. □

Theorem 4.40. (**Cipolla's Algorithm**)
In the field $\mathbb{Z}_p$, where $p \geq 3$ is prime, if a is a number with square root x, and b is a number such that $w^2 = b^2 - a$ has no square root, then:
(1) In $\mathbb{Z}_p[w]$, a has exactly two square roots $+x, -x \in \mathbb{Z}_p$.
(2) In $\mathbb{Z}_p[w]$, $(b+w)^{(p+1)/2}$ is a square root of a.

Proof. We may divide our proof into two parts.
Part 1: For all $z \in \mathbb{Z}_p[w]$:

$$\begin{aligned} z^2 = a &\iff (z-x)(z+x) = 0 \\ &\iff z - x = 0 \text{ or } z + x = 0 \\ &\iff z = +x \text{ or } z = -x \end{aligned}$$

Hence, a has exactly two square roots $+x, -x \in \mathbb{Z}_p$.

Part 2: Note that:

$$\begin{aligned}(b+w)^{p+1} &= (b+w)^p(b+w)\\ &= (b^p+w^p)(b+w)\\ &= (b-w)(b+w)\\ &= b^2-w^2\\ &= a\end{aligned}$$

Hence, $(b+w)^{(p+1)/2}$ is a square root of a. In addition, it is real.
Quod. Erat. Demonstrandum. □

References

[1] H. Ren, “Template for math notes,” 2021.