Preliminaries

We define the natural numbers $\mathbb{N}$ to be the strictly positive integers. That is, $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$. We additionally define $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Unless otherwise stated, all rings are commutative and contain a 1.

Given a ring R and two ideals I and J of R, define their sum and product as follows:

$$I + J = \{a + b : i \in a \text{ and } b \in J\},$$

and

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k : a_k \in I, b_k \in J, \text{ and } n \in \mathbb{N} \right\}.$$

We can generalize the product of ideals to finite collections of ideals. Let $I_1, I_2, \ldots, I_m$ be ideals of a ring R, then we define their product as follows:

$$I_1 I_2 \cdots I_m = \left\{ \sum_{k=1}^{n} \left(\prod_{l=1}^{m} a_{k,l} \right) : a_{k,l} \in I_k \text{ and } n \in \mathbb{N} \right\}$$

As a special case, the power ideal I^m is defined for $m \in \mathbb{N}$ as follows:

$$I^m = \left\{ \sum_{k=1}^{n} \left(\prod_{l=1}^{m} a_{k,l} \right) : a_{k,l} \in I \text{ and } n \in \mathbb{N} \right\}$$

Given a ring R and an arbitrary indexing set I, we define $R^{(I)}$ as the set of collections $\{a_i\}_{i \in I}$ of elements of R such that $a_i = 0$ for almost all $i \in I$. We can endow this set with an R-module structure by defining componentwise addition and scalar multiplication.

We define $\delta_{i,j}$ as follows:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Additionally, for the R-module $R^{(I)}$, we define the elements $e_i = \{d_{i,j}\}_{j \in I}$ and denote $\{e_i\}_{i \in I}$ as the canonical basis for $R^{(I)}$.

Given an R-module M, it is understand that 0 serves as the identity element of the abelian group M.

1.1 Divisibility in Principal Ideal Rings

Proposition 1.1: $\mathbb{Z}$ is a principal ideal domain.

Proof: Let I be a nonzero ideal in $\mathbb{Z}$, then we can choose a nonzero element $b \in I$. If $b < 0$, then $b^2 > 0$ and I has a positive element, thus without loss of generality we can assume $b > 0$. By the well ordering principle, we can also assume that b is minimal among the positive integers in I. Now, fix an arbitrary element $x \in I$. Since $\mathbb{Z}$ is a Euclidean domain, we have unique integers q and r such that $x = qb + r$, and where $0 \leq r < b$. Consequently, we have that $r = x - qb \in I$ since I is closed under addition. If $r > 0$, then we have found a positive integer in I that is less than b, a contradiction to our assumption, hence we must have $r = 0$. This shows that all elements in I are multiples of b, and thus $I = (b)$ and is a principal ideal. ■

Proposition 1.2: If K is a field, then $K[X]$ is a principal ideal domain.

Proof: Fix a nonzero ideal I in $K[X]$. Let d be the minimal nonzero degree of any element in I, and let b be an element in I with degree d. Letting x be any element in I, we can use the fact that $K[X]$ is a Euclidean domain to find unique elements $q, r \in I$ where $x = qb + r$, and where $0 \leq \deg(r) < \deg(b)$. By closure, we have that $r = x - qb \in I$, which combined with our assumption on $\deg(b)$ forces $\deg(r) = 0$. Thus, any element $x \in I$ is a multiple of b, meaning that $I = (b)$ and is thus principal. ■

1.2 Diophantine Equations

Theorem 1.3: We have that $x, y, z \in \mathbb{N}$ satisfy the equation $x^2 + y^2 = z^2$ if and only if there exists an integer d and relatively prime integers u and v such that, after possible rearrangement of x and y:

$$x = d(u^2 - v^2), \quad y = 2duv, \quad \text{and} \quad z = d(u^2 + v^2).$$

Proof: The backwards direction is easy to see, as

$$x^2 + y^2 = [d(u^2 - v^2)]^2 + (2duv)^2 = d^2(u^4 - 2u^2v^2 + v^4) + d^2(4u^2v^2)$$

$$= d^2(u^4 + 2u^2v^2 + v^4) = d^2(u^2 + v^2)^2 = z^2.$$

Conversely, let $x, y, z \in \mathbb{N}$ satisfy the equation. We can, without loss of generality, assume that they are pairwise relatively prime, since otherwise we can divide out by their gcd. ▲

Theorem 1.4: There exist no integers $x, y, z \in \mathbb{N}$ that satisfy the equation

$$x^4 + y^4 = z^2.$$

Proof: ▲

Corollary 1.5: There exist no integers $x, y, z \in \mathbb{N}$ that satisfy the equation

$$x^4 + y^4 = z^4.$$

Proof: ▲

1.3 Lemmas on Ideals and Euler's ϕ-function

Proposition 1.6: Fix natural numbers q and n, and denote $\tilde{q}$ as the residue class $q + n\mathbb{Z}$. We have that the following are equivalent:

(a) $\gcd(q, n) = 1$

(b) $\tilde{q}$ is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$

(c) $\tilde{q}$ generates the additive group $\mathbb{Z}/n\mathbb{Z}$

As a corollary, we have that $\phi(n)$ is equal to the number of units in the ring $\mathbb{Z}/n\mathbb{Z}$, as well as the number of generators of the additive group $\mathbb{Z}/n\mathbb{Z}$.

Proof: We will prove that (a) $\implies$ (b) $\implies$ (c) $\implies$ (a). We also choose q to be the unique representative of $\tilde{q}$ where $0 \leq q \leq n - 1$.

First, assume (a). By Bezout's lemma, there exist integers x and y such that $qx+ny = 1$. We thus have that $qx \equiv 1 \pmod{n}$, which is equivalent to $\tilde{q} \cdot \tilde{x} = \tilde{1}$. This proves (a) $\implies$ (b), and so we now assume that $\tilde{q}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Choose $\tilde{x} \in \mathbb{Z}/n\mathbb{Z}$ such that $\tilde{q} \cdot \tilde{x} = \tilde{1}$, then for arbitrary $\tilde{a} \in \mathbb{Z}/n\mathbb{Z}$ we have $\tilde{a} = \tilde{a} \cdot \tilde{x} \cdot \tilde{q}$. This is equivalent to $\tilde{a} = (ax)\tilde{q}$, which shows that $\tilde{q}$ generates all elements in $\mathbb{Z}/n\mathbb{Z}$, and (b) $\implies$ (c). Finally, assume $\tilde{q}$ to be a generator for $\mathbb{Z}/n\mathbb{Z}$, then there exists an integer x where $x\tilde{q} = \tilde{1}$, but this means that $xq \equiv 1 \pmod{n}$. We can choose an integer y such that $xq - 1 = yn$, which implies that $xq - yn = 1$. By Bezout's lemma, this implies that $\gcd(q, n) = 1$, thus showing (c) $\implies$ (a) and completing the proof. ■

Lemma 1.7: Let R be a ring and let I and J be ideals of R such that $I + J = R$, then we have that $I \cap J = IJ$ and $R/IJ \cong R/I \times R/J$.

Proof: We have that $IJ \subseteq I$ since I absorbs multiplication from J. Similarly, $IJ \subseteq J$, and thus $IJ \subseteq I \cap J$. Fix an element $x \in I \cap J$. By assumption, $I + J = R$, and so there exist elements a and b in I and J, respectively, such that $a + b = 1$, hence we obtain the equality $x = xa + xb$. This means that x is an element of IJ, and thus $IJ \subseteq I \cap J$. A a result, we have $IJ = I \cap J$.

Next, we consider the ring homomorphism $\theta : R \to R/I \times R/J$, which we define as $\theta(a) = (a+I, a+J)$. Since $a+I = I$ and $a+J = J$ if and only if $a \in I \cap J$, we have that $\ker\theta = I \cap J = IJ$. This shows that, if $a+IJ$ and $b+IJ$ are equivalent elements of R/IJ, then $\theta(a) = \theta(b)$. We can thus define a function $\phi : R/IJ \to R/I \times R/J$, defined as $\phi(a + IJ) = \theta(a) = (a + I, a + J)$. It is easy to verify that ϕ is a homomorphism. Additionally, if $a \in \ker\theta$, then $\phi(a + IJ) = \theta(a) = (I, J)$, which shows that $\ker\phi = \{0 + IJ\}$, and thus ϕ is injective. Finally, fix $(y + I, z + J) \in R/I \times R/J$, and again take a and b as elements in I and J, respectively, such that $a + b = 1$. Defining the element $x \in R$ as $x = az + by$, we can see that

$$x \equiv by \equiv (1-a)y \equiv y - ay \equiv y \pmod{a},$$

as well as

$$x \equiv az \equiv (1-b)z \equiv z - bz \equiv z \pmod{b}.$$

This shows that

$$\phi(x + IJ) = \theta(x) = (x + I, x + J) = (y + I, z + I),$$

thus ϕ is surjective, hence an isomorphism, and $R/IJ \cong R/I \times R/J$. ■

Lemma 1.8: Let R be a ring and let $I_1, I_2, \ldots, I_n$ be ideals of R such that $I_i + I_j = R$ for all $1 \le i < j \le n$. We have that $A/I_1I_2\cdots I_n \cong A/I_1 \times A/I_2 \times \cdots \times A/I_n$.

Proof: The previous lemma proves the case for $n = 2$. We now use induction on n and assume the case for $n-1$ holds. Define the ideal $J = I_2I_3\cdots I_n$ in R. Note that for $2 \le k \le n$, we have $J \subseteq I_k$ and $I_1 + I_k = R$, thus we can find elements $a_k \in I_1$ and $b_k \in J$ such that $a_k + b_k = 1$, and thus

$$1 = \prod_{k=2}^{n}(a_k + b_k).$$

Using this we obtain the equality $1 = c + a_2a_3\cdots a_n$, where c is the sum of the terms in the product that contain at least one b_k. This implies that $c \in I_1$, and thus $1 = c + a_2a_3\cdots a_n \in I_1 + J$. Because $I_1 + J$ is an ideal that contains 1, we know that $I_1 + J = R$.

By the previous lemma, we have

$$A/I_1J \cong A/I_1 \times A/J,$$

and invoking the induction hypothesis, we can see that

$$A/J = A/I_2 I_3 \cdots I_n \cong A/I_2 \times A/I_3 \times \cdots \times A/I_n,$$

thus we have that

$$A/I_1 I_2 \cdots I_n = A/I_1 J \cong A/I_1 \times A/J \cong A/I_1 \times A/I_2 \times \cdots \times A/I_n,$$

completing the proof. ■

Proposition 1.9: Let m and n be relatively prime integers, then we have that $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof: By Bezout's lemma, there exist integers x and y such that

$$xm + yn = 1,$$

which means that the ideal $m\mathbb{Z} + n\mathbb{Z}$ contains 1, and thus is equal to $\mathbb{Z}$. Applying **Lemma 1.7**, we obtain

$$\mathbb{Z}/(mn)\mathbb{Z} = \mathbb{Z}/(m\mathbb{Z}n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

■

Corollary 1.10: If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Proof: We previously established that $\phi(mn)$ is equal to the number of units in $\mathbb{Z}/mn\mathbb{Z}$, and thus the number of units in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since an element $(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if a and b are units in their respective rings, we have exactly $\phi(m)\phi(n)$ choices for units in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, thus proving the equality. ■

Corollary 1.11: For fixed $n \in \mathbb{N}$, let $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ be its prime factorization, then we have that

$$\phi(n) = n \prod_{k=1}^{m} \left(1 - \frac{1}{p_k}\right).$$

Proof: Since powers of distinct primes are always relatively prime, we have that $p_i^{a_i}\mathbb{Z} + p_j^{a_j}\mathbb{Z} = \mathbb{Z}$ for all $1 \le i < j \le m$. Additionally, $\mathbb{Z}/n\mathbb{Z}$ has $\phi(n)$ units. Furthermore, we have that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z}p_2^{a_2}\mathbb{Z} \cdots p_m^{a_m}\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \mathbb{Z}/p_2^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{a_m}\mathbb{Z},$$

but the number of units in the right hand side is equal to $\phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_m^{a_m})$.

Thus, we have that

$$\phi(n) = \prod_{k=1}^{m} \phi(p_k^{a_k}) = \prod_{k=1}^{m} p_k^{a_k} - p_k^{a_k-1} = \prod_{k=1}^{m} p_k^{a_k}\left(1 - \frac{1}{p_k}\right) = \prod_{k=1}^{m} p_k^{a_k} \prod_{k=1}^{n}\left(1 - \frac{1}{p_k}\right)$$
$$= n\prod_{k=1}^{m}\left(1 - \frac{1}{p_k}\right).$$

■

1.4 Preliminaries on Modules

Proposition 1.12: Let R be a ring, I an indexing set, and M an R-module. Additionally, let $\{m_i\}_{i\in I}$ be a fixed collection of elements in M, and let $a = \{a_i\}_{i\in I}$ be an element in $R^{(I)}$. We have that the function $\phi : R^{(I)} \to M$, defined as

$$\phi(a) = \sum_{i\in I} a_i m_i,$$

is an R-module homomorphism. Furthermore, the following are true:

(a) $\{m_i\}_{i\in I}$ is linearly independent if and only if ϕ is injective

(b) $\{m_i\}_{i\in I}$ generates M if and only if ϕ is surjective

Proof: Let $a = \{a_i\}_{i\in I}$ and $b = \{b_i\}_{i\in I}$ be elements in $R^{(I)}$. We can see that

$$\phi(a+b) = \sum_{i\in I}(a_i + b_i)m_i = \sum_{i\in I} a_i m_i + \sum_{i\in I} b_i m_i = \phi(a) + \phi(b),$$

and for $r \in R$, we have that

$$\phi(ra) = \sum_{i\in I} r a_i m_i = r\sum_{i\in I} a_i m_i = r\phi(a).$$

Note that we can factor the r out of the sum since only finitely many terms are nonzero. Thus, we have shown that ϕ is an R-module homomorphism.

Next, assume that the m_i are linearly independent. Letting $a, b \in R^{(I)}$ where $\phi(a) = \phi(b)$, we see that

$$\sum_{i\in I} a_i m_i = \sum_{i\in I} b_i m_i,$$

and thus

$$\sum_{i\in I}(a_i - b_i)m_i = 0.$$

The linear independence of the m_i force $a_i - b_i = 0$ for all $i \in I$, hence $a_i = b_i$ and $a = b$, which shows the injectivity of ϕ. Conversely, assume ϕ is injective. It is easy to see that $\phi(0) = \{0\}_{i\in I}$, as

$$\phi(0) = \sum_{i\in I} 0m_i = 0.$$

Additionally, if we have $a \in R^{(I)}$ such that $\phi(a) = 0$, then by the injectivity of ϕ we have that $a = 0$, and thus $a_i = 0$ for all $i \in I$.

Moving on to (b), we assume that $\{m_i\}_{i\in I}$ generates M. This means that, for all $m \in M$, we have $m = \sum_{i\in I} a_i m_i$ for