Polynomials

Thaqib Mo.

December 1, 2020

1 Polynomials over a Field

Definition 1: Polynomials over a Field

Let F be a field then we define $F[x]$ to be the field of polynomials with coefficients in F to be

$$F[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \geq 0, a_i \in F \text{ for each } i\}$$

The degree of the polynomial $f \in F[x]$ is denoted by $\deg(f)$ is the largest index i such that $a_i \neq 0$

We can turn $F[x]$ into a commutative ring by defining the operations on it. For $f, g \in F[x]$ with $f = \sum_{i=0}^{n} a_ix^i$ and $g = \sum_{i=0}^{m} b_ix^i$

$$f + g = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x$$

$$fg = \sum_{i=0}^{m+n} c_ix^i$$

$$\text{Where for each } i \text{ we have } c_i = \sum_{j=0}^{i} (a_jb_{i-j})$$

Theorem 1

Let F be an field and $f, g \in F[x]$ be non zero polynomials. We have the following:

(1) If $f + g \neq 0$ then $\deg(f + g) \leq \max(\deg(f), \deg(g))$

(2) $\deg(fg) = \deg(f) + \deg(g)$

(3) $F[x]$ is an integral domain.

Proof. (1) Holds by definition of $f + g$.

(2) We have $fg = \sum_{i=0}^{m+n} c_ix^i$. All coefficients after x^{m+n} are zero so we have $\deg(f+g) \leq m+n$ the coefficient c_{n+m} is given by $c_{n+m} = \sum_{j=0}^{n+m} a_jb_{n+m-j} = a_0b_{n+m} + a_1b_{n+m-1} + \ldots a_{n+m}b_0$ Note that $a_j = 0$ when ever $j > m$ so all the terms after a_mb_n are zero. Similarly we have $b_{m+n-j} = 0$ when $j < m$. So All terms before a_mb_n are zero. Finally since $a_m, b_n \neq 0$ and F is an integral domain so $a_mb_n \neq 0$ so we have $\deg(fg) = n + m$

(3) Given the 2 results. If we have $f \neq 0$ and $g \neq 0$ Then f, g both have a degree and $\deg(fg) = \deg(f) + \deg(g)$. So $\deg(fg) \neq 0$, combined with the fact that $F[x]$ is a commutative ring we have that $F[x]$ is also an integral domain.

□

2 Polynomial Division with Remainder

Theorem 2

For any Field F the integral domain $F[x]$ has a division algorithm with divisor function deg. For any polynomials $f, g \in F[x]$ there are polynomials $q, r \in F[x]$ such that

$$f = gq + r$$

And either $r = 0$ or $\deg(r) < \deg(g)$

Proof. Consider the set

$$S = \{f - gq : q \in F[x]\}$$

If $0 \in S$ then we have $f = gq + 0$ and we are done. Otherwise we can look at the degree of all polynomials in S. Let r be the polynomial with the lowest degree. We have $r = f - gq$. Suppose we have $\deg(r) \geq \deg(g)$ and let $r = a_n x^n a_{n-1} x^{n-1} + \cdots$ and $g = b_n x^n b_{n-1} x^{n-1} + \cdots$. Since $b_m \neq 0$ and $b_m \in F$ we know that b_m^{-1} exists. Since we assumed $\deg r \geq \deg g$ we have $n \geq m$. So we consider the new polynomial

$$\begin{aligned} r_1 &= r - a_n b_m^{-1} x^{n-m} g \\ &= a_n x^n a_{n-1} x^{n-1} + \cdots - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots) \\ &= (a_{n-1} - a_n b_m^{-1} b_{m-1}) x^{n-1} \end{aligned}$$

So $\deg r_1 < \deg r$ but we have

$$\begin{aligned} r_1 &= r - a_n b_m^{-1} x^{n-m} g \\ &= f - gq - a_n b_m^{-1} x^{n-m} g \\ &= f - g(q - a_n b_m^{-1} x^{n-m}) \end{aligned}$$

So we have $r_1 \in S$ contradicting that r had minimum degree. $\square$

We can find q, r using the long division process.

Example 1. *We can find $q, r \in (\mathbb{Z}/3\mathbb{Z})[x]$ such that*

$$x^3 + x^2 + [1] = ([2]x^2 + [1])q + r$$

$$
\begin{array}{r|l}
 & \qquad\qquad\qquad\qquad\qquad\qquad\qquad [2]x+[2] \\
\hline
[2]x^2+[1] & [1]x^3+[1]x^2+[1]x+[1] \\
 & \quad -([1]x^3+[2]x) \\
\hline
 & \qquad\qquad [1]x^2 \qquad +[1]x+[1] \\
 & \qquad\qquad -([1]x^2 \qquad +[0]x+[2]) \\
\hline
 & \qquad\qquad\qquad [1]x-[1]=x+[2]
\end{array}
$$

This long division process directly leads to some important results for the roots of polynomials. If $f \in F[x]$ we define the evaluation of polynomial f at c to be

$$f(c) = a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n$$

c is a root of the polynomial if $f(c) = 0$. We can define a ring homomorphism called the *evaluation homomorphism* to be

$$\phi_c : F[x] \to F \ \ \phi_c(f) = f(c)$$

We can easily show that this is a ring homomorphism and it leads to the following theorem:

Theorem 3: Factor Theorem

Let $f \in F[x]$ and $c \in F$ where F is a field.

(1) c is the root if and only if $(x - c) \mid f$ in the integral domain $F[x]$. Moreover we have $\ker(\phi_c) = F[x](x - c)$ the ideal generated by $(x - c)$.

(2) If if non zero $n = \deg(f)$ then f has at most n roots in F.

Proof. (1) Suppose we have $(x - c) \mid f$ then there is some polynomial $q \in F[x]$ such that $f = (x - c)q$ so we get

$$\phi_c(f) = \phi_c((x - c)q) = \phi_c(x - c)\phi_c(q) = 0 \cdot q(c) = 0$$

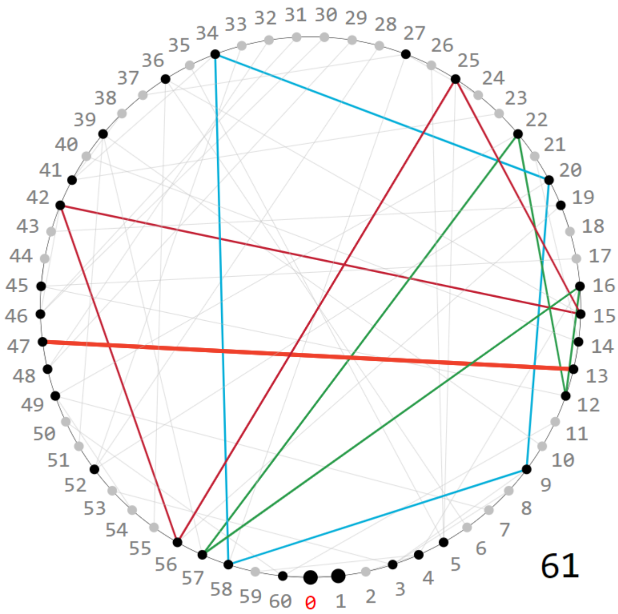
So c is a root of f. Conversely assume c is a root of f applying division with remainder with f we get $f = (x - c)q + r$ we either have $r = 0$ or $\deg r < \deg x - c = 1$ so we must have $r = r_0$. Applying ϕ_c gives $\phi_c(f) = \phi_c((x - c)q + r_0) = \phi_c(x - c)\phi_c(q) + r_0 = 0$ so we finally have $r_0 = 0$ therefore $(x - c) \mid f$. So we have $f(c) = 0 \iff (x-c) \mid f$ so this describes the principal ideal $F[x](x-c)$ for every $g \in F[x](x-c)$ we have $g(c) = 0$. Therefore $\ker \phi_c = F[x](x - c)$

(2) We can prove this by induction on $n = \deg(f)$ when we have $\deg(f) = 0$ then $f = f_0$ where $f_0 \neq 0$ so we have $f(c) = f_0 \neq 0$ for any $c \in F$, thus f has no roots. The same applies for $n = 1$ case.

Now suppose $\deg(f) = n + 1$ where $n \geq 1$ and assume for $k < n + 1$ we have at most k roots in F. If f has no roots we are done. Suppose c is a root applying the factor theorem we see that $f = (x - c)f_n$ for some polynomial f_n. We clearly have $\deg(f_n) = n$ due to the assumption we have f_n having at most n roots and for any $a \in F$ we have $f(a) = 0$ if and only if $(a - c)f_n(a) = 0$ So we have at most n possible values of a for $f_n(a) = 0$ and only 1 possible value for $a - c = 0$ therefore there are at most $n + 1$ roots.

□

Primitive Roots Modulo p



Lemma 1

Let G be a *finite abelian group* let $g \in G$ such that $o(g) = k$ is maximal then $h^k = e$ for all $h \in G$

Let $g \in G$ such that $o(g) = k$ is maximal. Assume we have some $h \in G$ such that $h^k \neq e$. Now consider $o(h)$ and k, we already know $h^k \neq e$ So we have

$$h^{o(h)} \neq h^k$$

This means we have $k \neq o(h) \bmod o(h)$ by Theorem 19.4. since $o(h)$ is finite. So we have $o(h) \nmid k - 0 \Rightarrow o(h) \nmid k$.

Consider the unique prime factorization of $|G|$

$$|G| = \prod_{i=1}^{a} p_i^{z_i}$$

With each p_i a prime number and $z_i \geq 1$. Since we have $k \mid |G|$ we can write k in terms of all p_i. We have

$$k = \prod_{i=1}^{a} p_i^{y_i}$$

With $0 \leq y_i \leq z_i$. We have a similar expression for $o(h)$

$$o(h) = \prod_{i=1}^{n} p_i^{x_i}$$

We can show that $o(h) = p^x n$ **and** $k = p^y n$ where m, n are positive integers not divisible by p and $x > y$

With $0 \leq x_i \leq z_i$. Since we have already established $o(h) \nmid k$ if we divide both of them we get

$$\begin{aligned} \frac{k}{o(h)} &= \frac{\prod_{i=1}^{a} p_i^{y_i}}{\prod_{i=1}^{n} p_i^{x_i}} \\ &= \frac{p_1^{y_1} p_2^{y_2} p_3^{y_3} \cdots}{p_1^{x_1} p_2^{x_2} p_3^{x_3} \cdots} \\ &= p_1^{y_1 - x_1} p_2^{y_2 - x_2} p_3^{y_3 - x_3} \cdots \end{aligned}$$

Assume we had for all i $x_i \leq y_i$ that would mean the above expression would be an integer so let

$$p_1^{y_1 - x_1} p_2^{y_2 - x_2} p_3^{y_3 - x_3} = a$$

That means we have $k = a o(h)$ which is a contradiction to $o(h) \nmid k$. So for some i we must have $x_i > y_i$. Let p_i be such that $x_i > y_i$ and we let $p_i = p$ and $x_i = x$ and $y_i = y$. Then without any loss of generality we write $o(h) = p^x n$ and $k = p^y m$ we let x, y maximum such integers so m, n are not divisive by p. We have shown such x, y, p, m, n must exist.

Since we have $o(h) = p^x m$ and $k = p^y n$ where $x > y$ and m, n are not divisible by p.
Now let $h_1 = h^m$. Now we need to find $o(h_1)$, since $h_1^{p^x} = (h^m)^{p^x} = h^{p^x m} = e$ so we have $o(h_1) \leq p^x$. Now let $o(h_1) = \ell$. Then $h_1^{\ell} = e$ that means we have $h^{m\ell} = e$. If we have $\ell < p^x$ that means we will have $\ell m < p^x m$ that is a contradiction to $o(h) = p^x m$. So we have $p^x \leq o(h_1)$. Combining both parts we have $o(h_1) = p^x$. Similarly let $g_1 = g^{p^y}$ we have $o(g_1) \leq n$ since $g_1^n = g^{p^y n} = e$. Now let $o(g_1) = \ell$ assume $\ell < n$ that leads to $g^{p^y \ell} = e$ and $p^y \ell < p^y n$ which is a contradiction. So we have $o(g_1) = n$

Now we need to find $o(h_1 g_1)$, let $o(h_1 g_1) = w$. We can prove the following proposition:

Proposition 1

If $a, b \in G$ with G being an finite abelian group and $o(a) = \ell$ and $o(b) = k$ with $\gcd(k, \ell) = 1$ then $o(ab) = k\ell$

Proof. Let $w = o(ab)$ we have $(ab)^{k\ell} = a^{k\ell}b^{k\ell}$ since G is abelian we get $a^{k\ell}b^{k\ell} = e^k e^\ell = e$. So we have $(ab)^w = (ab)^{k\ell}$. Since G is a finite abelian group we have $k\ell \equiv w \bmod w$ this means we have $w \mid k\ell$.
Using the same logic we have $(ab)^w = e$, and we have $e^\ell = ((ab)^w)^\ell = a^{w\ell}b^{w\ell} = eb^{w\ell}$. So we get $b^{w\ell} = e = b^k$ so again we have $k \mid w\ell$ since $\gcd(k, \ell) = 1$ applying Theorem 29.3 gives $k \mid w$. Applying the same argument with ℓ is symmetric and gives $\ell \mid w$. Since we have $\gcd(k, \ell) = 1$ applying Q4 leads to $k\ell \mid w$. Combining both $(k\ell \mid w)$ and $(w \mid k\ell)$ gives $w = k\ell$, therefore we have $o(ab) = k\ell$ □

Applying Proposition 1 to $o(h_1 g_1)$ since we have $o(h_1) = p^x$ and $o(g_1) = n$ and n does not divide p we have $\gcd(p^x, n) = 1$ and therefore $o(h_1 g_1) = p^x n$. Now since $x > y$ we have $p^x n > p^y n$ so we have $p^x n > k$ and $h_1 g_1 \in G$. Therefore the order of g is not maximal which is a contradiction, so we must have $h^k = e$ ■

Using the above lemma we have the following theorem

Theorem 4

Let F be a finite field then the group F^* of units of F is cyclic.

Proof. Since F^* is an finite abelian group we can choose $c \in F^*$ with maximal order. By the above lemma we have $a^k = 1$ for all $a \in F^*$. So the polynomial $x^k - 1$ has atleast $|F^*|$ distinct roots so we have $|F^*| \leq k$. Applying Lagrange's tells us that $k = o(c)$ must divide $|F^*|$ so we have $k \leq |F^*|$. So we have $k = |F^*|$. So there is an element $c \in F^*$ of order $|F^*|$ therefore $|F^*|$ is cyclic. □

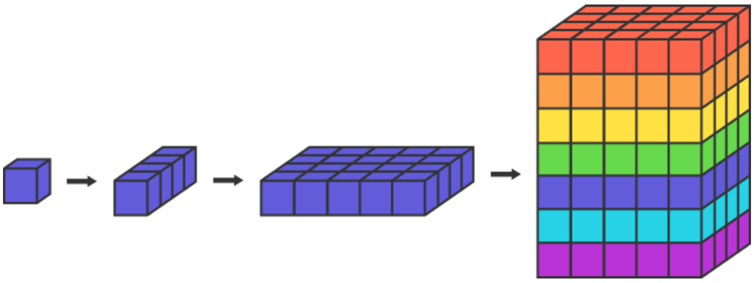
We can apply this to the finite field $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

Corollary 1

For any prime p the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic

Proof. For any prime p the group $(\mathbb{Z}/p\mathbb{Z})^*$ finite and the result follows from Theorem 4. □

3 Chinese Remainder Theorem



3.1 Classical version

The Chinese Remainder Theorem is the following general question for the set of equations:

$$\begin{cases} x \equiv a_1 \text{ mod } m_1 \\ x \equiv a_2 \text{ mod } m_2 \\ \vdots \\ x \equiv a_k \text{ mod } m_k \end{cases}$$

Where $m_1, m_2, \ldots m_k$ are positive integers and $a_1, a_2, \ldots a_k$ are integers. We want to find if there is some $x \in \mathbb{Z}$ satisfying them all?

In general the answer is no, since we have the counter example:

$$\begin{cases} x \equiv 1 \text{ mod } 2 \\ x \equiv 0 \text{ mod } 4 \end{cases}$$

The first equation requires x to be odd and the second requires x to be even so there are no solutions.

Some terminology: Integers a, b are called coprime if $\gcd(a, b) = 1$ and a set of integers $m_1, m_2, \ldots, m_k$ is called *pairwise* coprime if for any m_i, m_j with $i \neq j$ we have $\gcd(m_i, m_j) = 1$

Theorem 5: Chinese Remainder Theorem

Let $a_1, a_2, \dots a_k \in \mathbb{Z}$ and let $m_1, m_2, \dots m_k$ be pairwise coprime positive integers. Then the system

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

Has a solution $x \in \mathbb{Z}$ and this solution is unique in modulo $m_1 m_2 \cdots m_k$. If $y \in \mathbb{Z}$ is also a solution then

$$x \equiv y \bmod m_1 m_2 \cdots m_k$$

Proof. We can have a coordinate system with $(c_1, c_2, \dots c_k) \in (\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \mathbb{Z}/m_k\mathbb{Z})$ Then consider $b_1, b_2, \dots, b_k$ such that we have

$$\begin{cases} b_1 \equiv 1 \bmod m_1 \\ b_1 \equiv 0 \bmod m_2 \\ \vdots \\ b_1 \equiv 0 \bmod m_k \end{cases} \quad \begin{cases} b_2 \equiv 0 \bmod m_1 \\ b_2 \equiv 1 \bmod m_2 \\ \vdots \\ b_2 \equiv 0 \bmod m_k \end{cases} \quad \begin{cases} b_k \equiv 0 \bmod m_1 \\ b_k \equiv 0 \bmod m_2 \\ \vdots \\ b_k \equiv 1 \bmod m_k \end{cases}$$

We can think of these as b_1 having the first coordinate 1 and the rest 0, similarly b_i will have the i^{th} coordinate 1 and the rest 0.

We can prove that such a b_1 exists. Since $b_1 \equiv 0 \bmod m_i$ for $2 \le i \le k$ we must have $m_2 m_3 \dots m_k \mid b_1$ so let

$$M_1 = m_2 m_3 \dots m_k$$

So if we take $b_1 = c_1 M_1$ for some integer c_1 then we satisfy $b_1 \equiv 0 \bmod m_i$ for $2 \le i \le k$. We also need $b_1 \equiv 0 \bmod m_1$ since $c_1 M_1 \equiv 1 \bmod m_1$ c_1 must be a multiplicative inverse of M_1 for multiplicative inverse to exist we must have $\gcd(M_1, m_1) = 1$. Suppose $\gcd(M_1, m_1) \ne 1$ then M_1, m_1 share a prime factor that means that prime factor must be a factor of some m_i contradicting that they are pairwise coprime. So we must have $\gcd(M_1, m_1) = 1$ and such b_1 exists.

Similarly for $2 \le i \le k$ we can take $M_i = \prod_{j \ne i} m_j$ then from a similar argument above we can find all $b_i, 2 \le i \le k$. So such b_i must exist. Now we can use them to build the solution.

Let

$$x = \sum_{i=1}^{k} a_i b_i$$

For modulo m_1 we have

$$x = a_1b_1 + a_2b_2 + \cdots + a_kb_k \bmod m_1$$
$$x = a_1(1) + a_2(0) + \cdot a_k(0) \bmod m_1$$
$$x \equiv a_1 \bmod m_1$$

Similarly for all $b_i, 2 \leq i \leq k$ we have $x \equiv a_i \bmod m_i$ using the same argument. So this proves the existence of a solution.

Now for uniqueness, suppose x, y are both solutions. Then we have

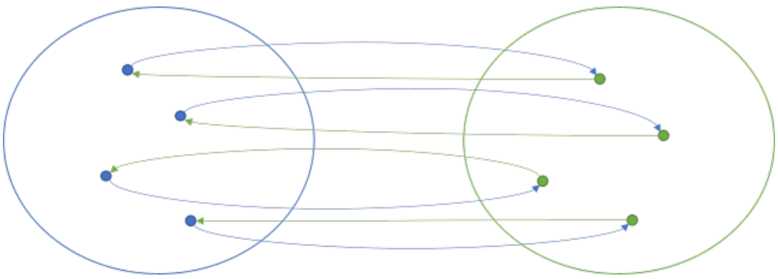
$$x \equiv y \mod m_i \; 1 \leq i \leq k$$

So we have $m_1 \mid x - y$ and $m_2 \mid x - y$ and $\gcd(m_1, m_2) = 1$ for so we have $m_1m_2 \mid x - y$. Since the primes are pairwise we have $\gcd(m_1m_2, m_3) = 1$ leading to $m_1m_2m_2 \mid x-y$ repeating this process gives $m_1m_2 \cdots m_k \mid x-y$ by definition we have

$$x \equiv y \bmod m_1m_2 \cdots m_k$$

□

3.2 Ring Theory Version



In the classical version the solution was unique in $\mathbb{Z}/m_1m_2 \cdots m_k\mathbb{Z}$ and since we built the correspondence between $(\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \mathbb{Z}/m_k\mathbb{Z})$ and $\mathbb{Z}/m_1m_2 \cdots m_k\mathbb{Z}$ we can lift this to a correspondence between product of rings.

For 2 rings to have the same structure we have the notion of isomorphism.

Definition 2: Isomorphism

A homomorphism $\phi : R \to S$ is called an *isomorphism* if ϕ is also a bijection.

Alternatively we can also show for $\phi : R \to S$ to be an isomorphism we can show there is an homomorphism $\psi : S \to R$ such that $\phi \circ \psi = \text{id}_S$ and $\psi \circ \phi = \text{id}_R$ where id_R , id_S are the identity maps on R, S.

If there is an isomorphism between 2 rings R, S then we say that the rings are isomorphic and we write $R \cong S$ isomorphic rings behave in the same way in all ring-theoretic respects.

Theorem 6: Chinese Remainder theorem (Ring Theory)

Suppose $m_1, m_2, \ldots, m_k$ are pairwise co prime then there is a isomorphism

$$\mathbb{Z}/m_1 m_2 \ldots m_k\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cdots \mathbb{Z}/m_k\mathbb{Z})$$

Proof. We construct an homomorphism and then prove it is a bijection. Using the coset notation the homomorphism is

$$\phi(m_1 m_2 \ldots m_k\mathbb{Z} + x) = (m_1\mathbb{Z} + x, m_2\mathbb{Z} + x, \ldots, m_k\mathbb{Z} + x)\,,$$

This map is well defined, consider if we have

$$m_1 m_2 \ldots m_k\mathbb{Z} + x = m_1 m_2 \ldots m_k\mathbb{Z} + y$$

Then $m_1 m_2 \ldots m_k \mid (x - y)$. In particular since all m_i are relatively prime we have $m_i \mid (x - y)$ so $m_i\mathbb{Z} + x = m_i\mathbb{Z} + y$ this means ϕ is well defined. The preservation of identity, addition and multiplication is trivial.
We show that ϕ is an injection. From Theorem 8 in (groups) showing $\ker(\phi) = \{m_1 m_2 \ldots m_k + 0\}$ means we can conclude ϕ is injective. Suppose we have x such that

$$\phi(m_1 m_2 \ldots m_k\mathbb{Z}) = (m_1\mathbb{Z} + 0, m_2\mathbb{Z} + 0, \ldots, m_k\mathbb{Z} + 0)$$

Then x satisfies

$$\begin{cases} x \equiv 0 \text{ mod } m_1 \\ x \equiv 0 \text{ mod } m_2 \\ \vdots \\ x \equiv 0 \text{ mod } m_k \end{cases}$$

Clearly 0 is a solution and by the uniqueness of solution in the classical version means it is the only solution in $\mathbb{Z}/m_1 m_2 \ldots m_k\mathbb{Z}$. So $\ker\phi$ is the zero ideal and we can conclude ϕ is injective.
For surjective suppose we have

$$(\mathbb{Z}m_1 + a_1, \mathbb{Z}m_2 + a_2, \ldots, \mathbb{Z}m_k + a_k) \in (\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cdots \mathbb{Z}/m_k\mathbb{Z})$$

By classical version there is x such that

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

So we always have x such that

$$\phi(\mathbb{Z}m_1m_2\dots m_k + x) = (\mathbb{Z}m_1 + a_1, \mathbb{Z}m_2 + a_2, \dots, \mathbb{Z}m_k + a_k)$$

Proving ϕ is also a surjection therefore a bijection and an isomorphism.

$\square$

4 Field of Fractions and Localization

4.1 Constructing Q

We know that every subring of a field is an intregral domain. The converse also holds, every integral domain is a subring of a field. To construct the ring $\mathbb{Q}$ from $\mathbb{Z}$ we specify $\frac{a}{b} \in \mathbb{Q}$ so we are actually specifying an ordered pair of integers (a, b) but we cannot have $b = 0$ and some ordered pairs can represent the same fraction like $(1, 2)$ and $(3, 6)$

We can define a relation $\sim$ on the set $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ with $(a, b) \sim (c, d)$ if $ad = bc$. We can do this for any ring in general and properties of $\mathbb{Z}$ are not very important to show this is an equivalence relation.

Proposition 2

Let R be an integral domain. We define $\sim$ on $R \times (R \setminus \{0\})$. We have $(a, b) \sim (c, d)$ if $ad = bc$. Then $\sim$ is an equivalence relation and the set of equivalence classes is denoted by $Q(R)$

Proof.

- **Reflexivity** We have $(a, b) \sim (a, b)$ since $ab = ba$
- **Symmetry** Suppose we have $(a, b) \sim (c, d)$ then we have $ad = bc$ This implies we also have $cb = da$ this means $(c, d) \sim (a, b)$
- **Transitivity** Suppose we have $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. By definition we have $ad = bc$ and $cf = de$. We multiply $ad = bc$ both sides by f

$$ad = bc$$
$$(ad)f = (bc)f$$
$$adf = b(cf) = b(de)$$

  Since R is an integral domain and $d \neq 0$ we have $af = be$ leading to $(a, b) \sim (e, f)$

$\square$

So we can say $\mathbb{Q} = Q(\mathbb{Z})$ where $[(a, b)]$ represents the fraction $\frac{a}{b}$ using the addition in $\mathbb{Q}$ we can define $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ and set $[(a, b)] + [(c, d)] = [(ad+bc, bd)]$. Similarly we have multiplication $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$. This procedure generalizes to arbitrary integral domains

Proposition 3

Let R be an integral domain we define $+, \cdot$ on $Q(R)$ by taking

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$
$$[(a,b)] \cdot [(c,d)][(ac, bd)]$$

Then $Q(R), +, \cdot$ is a field with these binary relations.

Prove later

Theorem 7

Let R be an integral domain. R is isomorphic to the sub ring $R_0 = \{\frac{r}{1} : r \in R\}$ of $Q(R)$ Identifying R with the subring R_0. Every non zero element of R has an inverse in $Q(R)$ and every element of $Q(R)$ $\frac{a}{b}$ can be written as ab^{-1}

Proof. To show that R_0 is a subring, we use the subring test. Clearly we have $\frac{1}{1} \in R_0$. Now assume we have $\frac{a}{1}, \frac{b}{1} \in R_0$ we have

$$\frac{a}{1} - \frac{b}{1} = \frac{a-b}{1} \in R_0$$
$$\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} \in R_0$$

So R_0 is a subring. Next we define $\sigma : R \to R_0$ by $\sigma(r) = \frac{r}{1}$ then we have

$$\sigma(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \sigma(r) + \sigma(s)$$
$$\sigma(rs) = \frac{rs}{1} = \frac{r}{1} \cdot \frac{s}{1} = \sigma(r)\sigma(s)$$

So σ is a ring homomorphism. Finally to check if σ is injective we can use the kernel theorem. Suppose we have $r \in R$ such that $\sigma(r) = 0$ by definition we have $(r,1) = (0,1)$ which means we have $r = 0$. Thus $\ker \sigma = \{0\}$ meaning ϕ is injective. Surjective is trivial since for any $\frac{r}{1} \in R_0$ we have $\sigma(r) = \frac{r}{1}$

So R_0 is isomorphic to R and we can identify R with R_0 via this isomorphism. Every non zero element of R has an inverse in $Q(R)$ since $Q(R)$ is a field by proposition 3. Also for any $a, b \in R$ we have $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = ab^{-1}$ □

4.2 Localization

Definition 3: Multiplicative set

Let R be an integral domain. A non empty subset $S \subseteq R$ is called multiplicative if $1 \in S$ and S is closed under multiplication.

We constructed the field of fractions as equivalence classes in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. We can generalized this to setting the denominators to specific multiplicative sets. $\mathbb{Z} \setminus \{0\}$ is clearly a multiplicative set but we can also do smaller sets like odd or even numbers.

Definition 4: Localization

Given an integral domain R and the multiplicative set $S \subseteq R$ we can form a new ring called the *localization* of R at S, denoted by

$$S^{-1}R$$

The elements are equivalence classes of ordered pairs $R \times S$ under the relation $\sim$ given by $(a, b) \sim (c, d)$ if $ad = bc$

The rules of addition and multiplication are same as $Q(R)$ but $S^{-1}R$ may not be a field. However R is still isomorphic to $S^{-1}R$ and every element in S has an inverse in $S^{-1}R$