8. Rings. Polynomials. Fields.

A. Ushakov

MA503, November 2, 2022

Contents

Our main goal is to describe structure of finite fields. But before we can do that we need to discuss a number of things.

- Some properties of finite abelian groups.
- Ring. General properties of rings.
- Field.
- Zero divisors and integral domains.
- Characteristic.
- Polynomial ring $F[x]$.
- Polynomial division with remainder.
- Polynomial zeros.
- Polynomial GCD.
- Euclidean lemma for polynomials.

Some properties of finite abelian groups

Suppose that $g_1 \in G_1$ and $g_2 \in G_2$ have finite order. Then the order of $(g_1, g_2) \in G_1 \times G_2$ is $\operatorname{lcm}(|g_1|, |g_2|)$.

$$
\begin{aligned}
\forall k \quad (g_1, g_2)^k = (e_1, e_2) \quad &\Leftrightarrow \quad (g_1^k, g_2^k) = (e_1, e_2) \\
&\Leftrightarrow \quad g_1^k = e_1 \text{ and } g_2^k = e_2 \\
&\Leftrightarrow \quad |g_1| \text{ divides } k \text{ and } |g_2| \text{ divides } k.
\end{aligned}
$$

Hence, the least positive number k satisfying $(g_1, g_2)^k = (e_1, e_2)$ is $\operatorname{lcm}(|g_1|, |g_2|)$.

$|\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}| = m_1 \ldots m_k$.

By definition of Cartesian product.

If $\gcd(m, n) = 1$, *then* $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}$.

- $|1| = n$ in $\mathbb{Z}_n$;
- $|1| = m$ in $\mathbb{Z}_m$;
- Hence, $|(1, 1)| = \operatorname{lcm}(m, n) = mn$, which means that $\mathbb{Z}_n \times \mathbb{Z}_m = \langle (1, 1) \rangle$.

Thus, $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}$.

Some properties of finite abelian groups – 2

If $\gcd(m_i, m_j) \neq 1$, *then* $\operatorname{lcm}(m_1, \dots, m_k) < m_1 \dots m_k$.

Recall the formula $\operatorname{lcm}(a, b) = \frac{a \cdot b}{\gcd(a,b)}$.

If $\gcd(m_i, m_j) \neq 1$, *then* $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$ *is not cyclic.*

By Lagrange theorem, $|\alpha_i|$ divides m_i for any $\alpha_i \in \mathbb{Z}_{m_i}$ and hence

$$|(\alpha_1, \dots, \alpha_k)| = \operatorname{lcm}(|\alpha_1|, \dots, |\alpha_k|) \leq \operatorname{lcm}(m_1, \dots, m_k) < m_1 \dots m_k.$$

$\mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_n^{r_n}}$ *is cyclic* $\Leftrightarrow$ $p_i \neq p_j \quad \forall i \neq j$.

Ring

A **ring** *is a set R with two binary operations $+$ and $\cdot$, called* **addition** *and* **multiplication***, that satisfy the following axioms:*

(R1) *$(R,+)$ is an abelian group with identity denoted by 0.*

(R2) *Multiplication is associative and R contains 1 (***unity***).*

(R3) $(a+b)c = ac + bc$ *and* $c(a+b) = ca + cb$.

The following are rings:

- The **zero ring** $R = \{0\}$.
- $(\mathbb{Z}, +, \cdot)$ – integers;
- $(\mathbb{Q}, +, \cdot)$ – rational numbers;
- $(\mathbb{R}, +, \cdot)$ – real numbers;
- $(\mathbb{C}, +, \cdot)$ – complex numbers.
- $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ with

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

The following are rings:

- $(\mathbb{Z}_n, +, \cdot)$.
- $\{a + bi \mid a, b \in \mathbb{Z}\}$ **Gaussian integers**.
- $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.
- The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries.

The following are not rings:

- $(\mathbb{N}, +, \cdot)$.
- $(2\mathbb{Z}, +, \cdot)$.

A subset $S \subseteq R$ is a **subring** *of a ring R if $(S, +, \cdot)$ is a ring. We write $S \leq R$.*

Rings: general properties

$0a = a0 = 0.$

$$a \cdot 1 + a \cdot 0 = a \cdot (1 + 0) = a \cdot 1 \quad \Rightarrow \quad a \cdot 0 = 0.$$

$a(-b) = (-a)b = -(ab).$

$$ab + a(-b) = a(b - b) = a0 = 0 \quad \Rightarrow \quad -(ab) = a(-b).$$

$(-a)(-b) = ab.$

Multiplicative identity is unique.

$$\begin{array}{ll} \forall a & 1 \cdot a = a \cdot 1 = a \\ \forall a & 1' \cdot a = a \cdot 1' = a \end{array} \quad \Rightarrow \quad 1 = 11' = 1'.$$

Multiplicative inverse is unique (when exists).

$$\begin{array}{ll} \forall a & b \cdot a = a \cdot b = 1 \\ \forall a & c \cdot a = a \cdot c = 1 \end{array} \quad \Rightarrow \quad c = cab = b.$$

Let R be a ring in which $1 = 0$. Then R is the zero ring.

$$a = a \cdot 1 = a \cdot 0 = 0.$$

Field

A ring R is a **commutative** *if $\cdot$ is commutative.*

All rings in our course are commutative!

We say that $b \in R$ is a **multiplicative inverse** *of $a \in R$ if $ab = 1$, in which case b is denoted by a^{-1}.*

$a \in R$ is a **unit** *if it has a multiplicative inverse in R.*

A **field** *is a commutative ring in which* **every non-trivial element is a unit**.

The following are fields:

- $(\mathbb{Q}, +, \cdot)$ – rational numbers;
- $(\mathbb{R}, +, \cdot)$ – real numbers;
- $(\mathbb{C}, +, \cdot)$ – complex numbers.
- $(\mathbb{Z}_n, +, \cdot)$ is a field $\Leftrightarrow$ n is prime.

The following are fields:

- $\{a + bi \mid a, b \in \mathbb{Q}\}$.
- $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

The following are not fields:

- The zero ring $R = \{0\}$.
- $(\mathbb{Z}, +, \cdot)$.

A subset $S \subseteq F$ is a **subfield** *of a field F if $(S, +, \cdot)$ is a field. We write $S \leq F$.*

Zero divisors and integral domains

(No zero divisors property for a ring R)

$ab = 0 \quad \Rightarrow \quad a = 0$ **or** $b = 0$ *for every* $a, b \in R$.

That property holds for classical rings and fields $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

We say that $a \neq 0$ is a **zero divisor** *in R if for some $b \neq 0$, $ab = 0$.*

That property do not hold in general. For instance, $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

Definition

An **integral domain** (ID) is a non-zero commutative ring with no zero divisors.

Every field is an integral domain.

$$a \neq 0 \text{ and } ab = 0 \quad \Rightarrow \quad b = (a^{-1}a)b = a^{-1}(ab) = 0.$$

Every finite integral domain is a field.

$\{a_1, \ldots, a_n\} \xrightarrow{*a} \{aa_1, \ldots, aa_n\}$ is a bijection.

Cancellation laws (can be skipped)

For classical rings and fields $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the following holds:

- **(Right cancellation law)** For any a, b, c if $c \neq 0$ and $ac = bc$ then $a = b$.
- **(Left cancellation law)** For any a, b, c if $c \neq 0$ and $ca = cb$ then $a = b$.

Proposition

Cancellation laws hold in R $\quad \Leftrightarrow \quad$ R has no zero divisors.

"$\Rightarrow$" (Contrapositive) Suppose that $a \cdot b = 0$ for some $a \neq 0, b \neq 0$. Then

$$a \cdot b = 0 = 0 \cdot b \not\Rightarrow a = 0$$

and the RCL does not hold.

"$\Leftarrow$" (Contrapositive) If the RCL does not hold for R. Then for some $a \neq b$ and $c \neq 0$ we have $ac = bc$. Then

$$0 = ac - bc = (a - b)c$$

Hence, c and $a - b$ are zero divisors.

Characteristic

For $a \in R$ and $n \in \mathbb{Z}$ define an element

$$n \cdot a = \begin{cases} \underbrace{a + \ldots + a}_{n \text{ times}} & \text{if } n > 0; \\ 0 & \text{if } n = 0; \\ \underbrace{(-a) + \ldots + (-a)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$$

Definition

The **characteristic** $\chi(R)$ of a ring R is the least $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ if such n exists, and 0 otherwise.

For instance, $\chi(\mathbb{Z}_n) = n$, $\chi(\mathbb{Z}) = 0$, $\chi(\mathbb{Q}) = 0$

Lemma (Freshman exponentiation)

If $\chi(F) = p$, then $(\alpha + \beta)^p = \alpha^p + \beta^p$ for every $\alpha, \beta \in F$.

By the binomial theorem

$$(\alpha + \beta)^p = \alpha^p + \binom{p}{1} \alpha^{p-1} \beta^1 + \ldots + \binom{p}{p-1} \alpha^1 \beta^{p-1} + \beta^p = \alpha^p + \beta^p$$

because for every $1 \leq s \leq p - 1$ the prime p divides $\binom{p}{s}$.

Polynomial over a ring

Fix a ring R and an indeterminate x (a formal symbol, a letter).

A **polynomial** *of degree n over R is a sum $p = \mathrm{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n}$, where $a_i \in R$ and $a_n \neq 0$. $R[x]$ is the set of all polynomials over R.*

- *degree n is denoted by $\deg(p)$;*
- *a_n is called the* **leading coefficient** *and denoted by $\mathrm{lc}(p)$;*
- *p is* **monic** *if $\mathrm{lc}(p) = 1$;*
- *a polynomial of the form a_nx^n is called a* **monomial***;*
- *a polynomial of degree 0 is called a* **constant polynomial***;*
- $\deg(0)$ *is not defined.*

For $a = \sum a_ix^i$ and $b = \sum b_ix^i$ define

$$\mathrm{a + b} = \sum \mathrm{(a_i + b_i)x^i} \quad \text{and} \quad \mathrm{a \cdot b} = \sum \mathrm{c_ix^i}, \text{ where } c_n = \sum^n a_ib_{n-i}.$$

Definition

$(R[x], +, \cdot)$ is a ring, called **the ring of polynomials over R**.

- $(x+1)(x+1) = x^2 + 1$ in $\mathbb{Z}_2[x]$
- $(x+1)(x+1) = x^2 + 2x + 1$ in $\mathbb{Z}_3[x]$
- $(x^2+x+1)(x^2+x+1) = x^4 + 2x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$

Polynomials: properties

$deg(p_1 p_2) \leq deg(p_1) + deg(p_2)$.

$$(a_n x^n + \ldots) \cdot (b_m x^m + \ldots) = a_n b_m x^{n+m} + \ldots + a_0 b_0.$$

$deg(p_1 p_2) = deg(p_1) + deg(p_2)$ if R is an ID.

$a_n \neq 0, \ \& \ b_m \neq 0 \quad \Rightarrow \quad a_n b_m \neq 0.$

If R is an ID, then $R[x]$ is an ID.

Because product of nontrivial polynomials is nontrivial.

$R[x]$ is not a field, even when R is a field.

x is never a unit in $R[x]$.

Division with remainder in $F[x]$

Let F be a field and $f(x), g(x) \in F[x]$, where $g(x) \neq 0$.

Definition (Polynomial division)

To divide $f(x)$ by $g(x)$ means to express $f(x)$ in the following form:

$$\mathrm{f(x) = q(x)g(x) + r(x)} \quad \text{and} \quad \mathrm{deg(r) < deg(g)}.$$

- $q(x)$ is called the **quotient** of division;
- $r(x)$ is called the **remainder** of division.

Theorem

For $f(x)$ and $g(x) \neq 0$ there are unique polynomials $q(x), r(x) \in F[x]$ satisfying

$$f(x) = q(x)g(x) + r(x) \quad \textit{and} \quad \deg(r) < \deg(g).$$

For instance, in $\mathbb{Z}_7[x]$, dividing $f(x) = x^6 + 3x^5 + 4x^2 - x + 2$ by $g(x) = x^2 + 2x - 3$ (using long division) we get $q(x) = x^4 + x^3 + x^2 + x + 5$ and $r(x) = -8x + 17$.

Definition

If $f(x) = g(x)q(x)$ for some $q(x) \in F[x]$, then we say that $g(x)$ **divides** $f(x)$ in $F[x]$ and write $g(x) \mid f(x)$.

Irreducible polynomial

Definition

$f(x) \in F[x]$ is **reducible** if $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in F[x]$. Otherwise, it is **irreducible**.

For instance, the following are irreducible in $\mathbb{Z}_2[x]$:

- x, $x + 1$,
- $x^2 + x + 1$,
- $x^3 + x + 1$, $x^3 + x^2 + 1$.

The following are irreducible in $\mathbb{Z}_3[x]$:

- x, $x + 1$, $x + 2$,
- $x^2 + 1$,

Polynomials: zeros

If F is a subfield of E, then E is a **field extension** *of F.*

Let E be a field extension of F.

Definition

We say that $\alpha \in E$ is a **zero** of $f(x) \in F[x]$ if $f(\alpha) = 0$.

Notice that $x^k - \alpha^k = (x-\alpha)(x^{k-1} + x^{k-2}\alpha + \ldots + x\alpha^{k-2} + \alpha^{k-1})$ for any $k \in \mathbb{N}$.

Proposition

$\alpha \in E$ is a zero of $f(x) \in F[x] \quad \Leftrightarrow \quad (x-\alpha)$ divides $f(x)$ in $E[x]$.

"$\Rightarrow$" $f(\alpha) = 0 \quad \Rightarrow \quad$
$$\begin{aligned} f(x) = f(x) - f(\alpha) &= a_n x^n + \ldots + a_0 - (a_n\alpha^n + \ldots + a_0) \\ &= a_n(x^n - \alpha^n) + \ldots + a_1(x-\alpha) \\ &= (x-\alpha)g(x). \end{aligned}$$

"$\Leftarrow$" $f(x) = (x-\alpha)g(x) \quad \Rightarrow \quad f(\alpha) = 0.$

α is a **zero of multiplicity** *k for $f(x)$ if $f(x) = (x-\alpha)^k g(x) \in E[x]$ and k is the greatest such power. A zero of multiplicity one is called* **simple**.

Polynomials: zeros

If α is a zero of $f(x) = g(x)h(x)$, then either α is a zero of $g(x)$, or α a zero of $h(x)$.

$$0 = f(\alpha) = g(\alpha)h(\alpha) \quad \Rightarrow \quad g(\alpha) = 0 \ \text{ or } \ h(\alpha) = 0.$$

Theorem (Number of zeros – case of a field)

A polynomial of degree n over a field F can have up to n distinct zeros in F.

If $\alpha_1, \dots, \alpha_{n+1}$ are distinct zero of $f(x)$, then

$$\begin{aligned} f(x) &= (x - \alpha_1)f_1(x) \\ &= (x - \alpha_1)(x - \alpha_2)f_2(x) \\ &\dots \\ &= (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_{n+1})f_n(x), \end{aligned}$$

which makes no sense, because the degree of the RHS is at least $n + 1$.

Corollary

The congruence $x^2 \equiv_p 1$ has exactly two solutions $x = \pm 1$.

Because computations modulo p is computations in $\mathbb{Z}_p$, which is a field.

A polynomial of degree n over a ring *can have more than n zeros. For instance, $x^2 - 1 \in \mathbb{Z}_{15}[x]$ has zeros $\{1, 4, 11, 14\}$.*

Polynomial GCD

Definition

Let $f(x), g(x) \in F[x]$. Define $\gcd(f(x), g(x))$ to be the **monic** polynomial of the highest degree that divides $f(x)$ and $g(x)$.

For instance, $\gcd(x^2+1, x^2+x+3) = x+2$ in $\mathbb{Z}_5[x]$.

Proposition (Such an object exists!)

If $f \neq 0$ or $g \neq 0$, then $\gcd(f, g)$ exists and is unique.

(Existence)

- Let $CD(f, g)$ be the set of all common divisors for f and g.
- $1 \in CD(f, g)$ and so $CD(f, g)$ is not empty.
- $h \in CD(f, g) \quad \Rightarrow \quad \deg(h) \leq \min(\deg(f), \deg(g))$.
- Hence, $CD(f, g)$ has a polynomial $h(x) = a_n x^n + \ldots$ of the highest degree.
- Then $\frac{h(x)}{a_n} \in CD(f, g)$ is a monic polynomial of the highest degree.

So, for f and g there is a monic polynomial of the highest degree that divides f and g.

(Uniqueness) To prove uniqueness we need the Euclidean lemma.

Euclidean lemma for polynomials

(Euclidean lemma for polynomials)

If $f(x) = q(x)g(x) + r(x)$*, then* $\gcd(f(x), g(x)) = \gcd(r(x), g(x))$.

Find $\gcd(f, g)$ *for* $f(x) = x^5 + 2x^3 + x + 1$ *and* $g(x) = x^4 + x + 2$ *in* $\mathbb{Z}_3[x]$.

$$\begin{aligned} f(x) &= xg(x) + 2x^3 + 2x^2 + 2x + 1 \\ g(x) &= (2x+1)(2x^3 + 2x^2 + 2x + 1) + 1 \end{aligned} \quad \Rightarrow \quad \begin{aligned} \gcd(f, g) &= \gcd(2x^3 + 2x^2 + 2x + 1, g) \\ &= \gcd(2x^3 + 2x^2 + 2x + 1, 1) = 1. \end{aligned}$$

I'd like to emphasize that this process can produce a non-monic polynomial $cx^k + \dots$*. To get a monic polynomial (gcd) simply multiply the result by* $\frac{1}{c}$.

Find $\gcd(f, g)$ *for* $f(x) = x^4 + 2x^3 + 4x^2 + 3x + 1$ *and* $g(x) = 2x^3 + 4x^2 + 4x$ *in* $\mathbb{Z}_5[x]$.

$$\begin{aligned} x^4 + 2x^3 + 4x^2 + 3x + 1 &= (3x) \cdot (2x^3 + 4x^2 + 4x) + (2x^2 + 3x + 1) \\ 2x^3 + 4x^2 + 4x &= (x+3) \cdot (2x^2 + 3x + 1) + (4x + 2) \\ 2x^2 + 3x + 1 &= (3x+3) \cdot (4x+2) + (0) \end{aligned} \quad \begin{aligned} \Rightarrow \gcd(g, f) &= \gcd(2x^2 + 3x + 1, 2x^3 + 4x^2 + 4x) \\ &= \gcd(4x + 2, 2x^2 + 3x + 1) \\ &= \gcd(0, 4x + 2) = 4x + 2 \end{aligned}$$

Dividing by 4 we get $\gcd(g, f) = x + 3$.

Bezout identity for polynomials

For any $f(x), g(x) \in F[x]$ there are $\alpha(x), \beta(x) \in F[x]$ satisfying $\gcd(f(x), g(x)) = \alpha(x)f(x) + \beta(x)g(x)$.

Example for $f(x) = x^5 + 2x^3 + x + 1$ and $g(x) = x^4 + x + 2$ in $\mathbb{Z}_3[x]$.

$$\begin{aligned} f(x) &= xg(x) + 2x^3 + 2x^2 + 2x + 1 \quad &\Rightarrow \quad \gcd(f, g) &= \gcd(2x^3 + 2x^2 + 2x + 1, g) \\ g(x) &= (2x+1)(2x^3 + 2x^2 + 2x + 1) + 1 & &= \gcd(2x^3 + 2x^2 + 2x + 1, 1) = 1. \end{aligned}$$

Then

$$\begin{aligned} 1 &= g(x) - (2x+1)(2x^3 + 2x^2 + 2x + 1) \\ &= g(x) - (2x+1)(f(x) - xg(x)) \\ &= (1 + x(2x+1))g(x) - (2x+1)f(x) \\ &= (2x^2 + x + 1)g(x) - (2x+1)f(x). \end{aligned}$$

Hence, $\alpha(x) = -(2x+1)$ and $\beta(x) = 2x^2 + x + 1$.

(Uniqueness of gcd)

Let $h_1(x), h_2(x)$ be two monic common divisors for $f(x), g(x) \in F[x]$ of the highest possible degree. Then $h_1 = h_2$.

- (Assumption) $h_1 \mid f$ and $h_1 \mid g \quad \Rightarrow \quad f = q_1 h_1$ and $g = q_2 h_1$.
- (Bezout) $h_2 = \alpha \cdot f + \beta \cdot g$ for some $\alpha, \beta \in F[x]$.
- Hence, $h_2 = \alpha \cdot q_1 h_1 + \beta \cdot q_2 h_1 = h_1(\alpha \cdot q_1 + \beta \cdot q_2)$.
- Then $h_1 = h_2$, because h_1, h_2 are monic and of the same degree.

Bezout identity for polynomials: another example

Example for $f(x) = x^5 + 1$ *and* $g(x) = x^4 + x^2$ *in* $\mathbb{Z}_2[x]$.

$$
\begin{aligned}
x^5 + 1 &= (x) \cdot (x^4 + x^2) + (x^3 + 1) & \Rightarrow \gcd(x^4 + x^2, x^5 + 1) &= \gcd(x^3 + 1, x^4 + x^2) \\
x^4 + x^2 &= (x) \cdot (x^3 + 1) + (x^2 + x) & &= \gcd(x^2 + x, x^3 + 1) \\
x^3 + 1 &= (x + 1) \cdot (x^2 + x) + (x + 1) & &= \gcd(x + 1, x^2 + x) \\
x^2 + x &= (x) \cdot (x + 1) + (0) & &= \gcd(0, x + 1) = x + 1
\end{aligned}
$$

Hence,

$$
\begin{aligned}
x + 1 &= (x + 1) \cdot (x^2 + x) + (1) \cdot (x^3 + 1) \\
&= (x + 1) \cdot ((x^4 + x^2) - (x) \cdot (x^3 + 1)) + (1) \cdot (x^3 + 1) \\
&= (x^2 + x + 1) \cdot (x^3 + 1) + (x + 1) \cdot (x^4 + x^2) \\
&= (x^2 + x + 1) \cdot ((x^5 + 1) - (x) \cdot (x^4 + x^2)) + (x + 1) \cdot (x^4 + x^2) \\
&= (x^3 + x^2 + 1) \cdot (x^4 + x^2) + (x^2 + x + 1) \cdot (x^5 + 1)
\end{aligned}
$$

Hence, $\alpha(x) = x^2 + x + 1$ and $\beta(x) = x^3 + x^2 + 1$.