Summary

Thursday, March 12, 2020 6:20 PM

$\boxed{\mathbb{Z}_n}$ • $\mathbb{Z}_n^\times = \{[a]_n \mid \gcd(a,n) = 1\}$.

• Euler ϕ-function,

$$\phi(n) := |\{a \mid 1 \le a \le n,\ \gcd(a,n)=1\}|.$$

• $|\mathbb{Z}_n^\times| = \phi(n)$.

• $c_n : \mathbb{Z} \to \mathbb{Z}_n$, $c_n(a) = [a]_n$ is a ring homomorphism, and $\ker c_n = n\mathbb{Z}$.

• $\mathbb{Z}_n$ is a field $\Leftrightarrow$ $\mathbb{Z}_n$ is an integral domain

$\Leftrightarrow$ n is prime.

• (Chinese Remainder Theorem) If $\gcd(m,n)=1$, then

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

• If $\gcd(m,n)=1$, then $\phi(mn) = \phi(m)\phi(n)$.

• If p is prime, then $\phi(p^k) = p^k - p^{k-1}$.

$\mathbb{Z}_n$ was used to introduce rings, units, fields, integral domains, ring homomorphisms, kernel, and ring isomorphisms.

Summary

Thursday, March 12, 2020 7:46 PM

Characteristic

$\text{Char}(R) =$ smallest positive integer n such that $nx = 0 \ \forall x \in R$

if there is no such positive integer, $\text{char}(R) = 0$.

- R unital $\Rightarrow$ $\text{Char}(R) = \begin{cases} \text{the additive order of } 1 \text{ if finite} \\ 0 \quad \text{Otherwise.} \end{cases}$

- Suppose $R_1, \ldots, R_m$ are unital rings and $\text{char}(R_i) < \infty$.

  Then $\text{Char}(R_1 \times \cdots \times R_m) = \text{l.c.m.}(\text{Char}(R_1), \ldots, \text{Char}(R_m))$.

- If D is an integral domain, then

  $\text{Char}(D)$ is either 0 or a prime.

Integral domain

- Unital commutative non-trivial without zero-divisors.
- Cancellation law.
- Field $\Rightarrow$ integral domain. Converse is not true in general.
- Finite integral domain $\Rightarrow$ Field.
- Any integral domain has a field of fractions.

Summary

Thursday, March 12, 2020 7:58 PM

Universal Property of field of fractions.

Suppose D is an integral domain. Then we constructed

$$Q(D) = \{ a/b \mid a \in D,\ b \in D \setminus \{0\} \}.$$

⓪ $Q(D)$ is a field.

① $i: D \to Q(D)$, $i(a) = a/1$ is an injective ring homomorphism.

② Suppose $\theta: D \to F$ is an injective ring homomorphism and F is a field. Then $\tilde{\theta}: Q(D) \to F$,

$$\tilde{\theta}(a/b) := \theta(a)\theta(b)^{-1}$$

is a well-defined injective ring homomorphism.

We used this property to show $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$.

<u>Step 1.</u> $\mathbb{Q}[i]$ is a field.

<u>Step 2.</u> Get $\tilde{\theta}$ using the universal property.

<u>Step 3.</u> Show $\tilde{\theta}$ is surjective.

Summary

Thursday, March 12, 2020 8:07 PM

$\boxed{\text{Ring of polynomials}}$

. If D is an integral domain, then

$$\forall f, g \in D[x], \quad \deg(fg) = \deg f + \deg g.$$

. If D is an integral domain, then $D[x]$ is an integral domain.

. If D is an integral domain, then $D[x]^\times = D^\times$.

. Polynomial vs. functions. Based on Fermat's little theorem if p is prime, $\forall a \in \mathbb{Z}_p$, $a^p = a$; but $x^p \neq x$ as two polynomials.

. Evaluation map. $F \subseteq E$ and $\alpha \in E$

$$\phi_\alpha : F[x] \to E, \ \phi_\alpha(g(x)) = g(\alpha) \text{ is a ring hom.}$$

$$\ker(\phi_\alpha) = \{ g(x) \in F[x] \mid g(\alpha) = 0 \}.$$

. Long Division; existence. R: unital commutative $f, g \in R[x]$, the leading coeff. of g is a unit $\Rightarrow$ $\exists\, q, r \in R[x]$, (1) $f(x) = g(x)\, q(x) + r(x)$ (2) $\deg r < \deg g$.

Summary

Thursday, March 12, 2020 8:19 PM

Long division; uniqueness. Suppose D is an integral domain. $\forall f, g \in D[x]$, leading coeff. of D is a unit. Then there are unique $q, r \in D[x]$ s.t.

(1) $f(x) = g(x)\,q(x) + r(x)$ (2) $\deg r < \deg g$.

Factor Theorem. Suppose R is a unital commutative ring; $f(x) \in R[x]$, $a \in R$. Then

$$f(a) = 0 \iff \exists\, q(x) \in R[x],\ f(x) = (x-a)\,q(x).$$

Generalized Factor Theorem. Suppose D is an integral domain; $f(x) \in D[x]$. If $f(a_1) = \cdots = f(a_m) = 0$ and $a_i \neq a_j$ for $i \neq j$, then $\exists\, q(x) \in D[x]$ s.t.

$$f(x) = (x-a_1)\cdots(x-a_m)\,q(x).$$

This was used to show $x^p - x = x(x-1)\cdots(x-(p-1))$ in $\mathbb{Z}_p[x]$

We used this to prove Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. ($p$ is prime.) Later this was extended to all finite fields.

Summary

Thursday, March 12, 2020 8:31 PM

- Recalled binomial expansion $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$

where $\binom{n}{i} = \dfrac{n!}{i!\,(n-i)!}$. Used this to show that

if $\mathrm{Char}(R) = p$ is prime, then

$F_p : R \to R$, $F_p(a) := a^p$ is a ring homomorphism.

(This was an alternative way of proving Fermat's little theorem.)

$\boxed{\text{Algebraic numbers}}$

$\alpha \in \mathbb{C}$ is called algebraic if $\exists\, g(x) \in \mathbb{Q}[x] \setminus \{0\}$,

$g(\alpha) = 0$. Alternatively if $\ker(\phi_\alpha) \neq 0$.

To understand $\ker(\phi_\alpha)$ we started the study of ideals.

$\boxed{\text{Ideals and Factor rings}}$ R: commutative.

$\emptyset \neq I \subseteq R$ is called an ideal if

(1) $\forall x, y \in I$, $x - y \in I$, (2) $\forall x \in I$, $\forall r \in R$, $rx \in I$.

Summary

Thursday, March 12, 2020 8:44 PM

- If $I \triangleleft R$, then we constructed the factor ring R/I and showed $\pi: R \to R/I$, $\pi(r) := r+I$ is an onto ring homomorphism and $\ker(\pi) = I$.

The 1st Isomorphism Theorem.

Suppose $f: R \to S$ is a ring homomorphism. Then

(0) $\ker f \triangleleft R$, $\operatorname{Im}(f) \subseteq S$ is a subring.

(1) $\bar{f}: R/\ker f \to \operatorname{Im}(f)$, $\bar{f}(r + \ker f) := f(r)$

is a well-defined ring homomorphism.

Ideals generated by $a_1, \dots, a_n$; principal ideals; PID.

The smallest ideal that contains $a_1, \dots, a_n$ is denoted by $\langle a_1, \dots, a_n \rangle$ and it is

$$\{r_1 a_1 + \cdots + r_n a_n \mid r_1, \dots, r_n \in R\}$$

when R is a unital commutative ring.

- $\langle a \rangle = Ra$ is called a principal ideal.

Summary

Thursday, March 12, 2020 8:56 PM

. An integral domain D is called a Principal Ideal Domain (PID) if all of its ideals are principal.

. <u>Theorem</u> $\mathbb{Z}$ and $F[x]$ are PIDs if F is a field.

Theorems on algebraic numbers $\alpha \in \mathbb{C}$ algebraic.

(Minimal polynomial). $\exists!$ monic irreducible $m_\alpha(x) \in \mathbb{Q}[x]$ s.t.

$$\ker \phi_\alpha = \langle m_\alpha(x) \rangle .$$

- $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$ implies $m_\alpha(x) \mid f(x)$.
- If $p(x) \in \mathbb{Q}[x]$ is monic and irreducible and

$$p(\alpha) = 0, \text{ then } m_\alpha(x) = p(x) .$$

$\left(\mathbb{Q}[\alpha] := \operatorname{Im} \phi_\alpha\right)$ Suppose $\deg m_\alpha = d$.

- $\mathbb{Q}[\alpha]$ is the $\mathbb{Q}$-span of $1, \alpha, \dots, \alpha^{d-1}$; that means

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1} \mid a_0, \dots, a_{d-1} \in \mathbb{Q}\} .$$

- $1, \alpha, \dots, \alpha^{d-1}$ are $\mathbb{Q}$-linearly independent; that means

$$\left.\begin{array}{c} b_0 + b_1\alpha + \dots + b_{d-1}\alpha^{d-1} = c_0 + c_1\alpha + \dots + c_{d-1}\alpha^{d-1} \\ b_i, c_i \in \mathbb{Q} \end{array}\right\} \Rightarrow b_i = c_i \ \forall i .$$

Summary

Thursday, March 12, 2020 9:08 PM

- $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/\langle m_\alpha(x)\rangle$ (using the 1^{st} isomorphism theorem.)
- $\mathbb{Q}[\alpha]$ is a field.

To prove the last item we studied maximal ideals.

$\boxed{\text{Maximal and Prime Ideals}}$

$I \triangleleft R$ is called a maximal ideal if

(1) I is a proper ideal; that means $I \neq R$,

(2) $\left.\begin{array}{l} I \subsetneq J \\ J \triangleleft R \end{array}\right\} \Rightarrow J = R$.

<u>Theorem</u>. I is maximal $\Leftrightarrow$ R/I is a field.

- $I \triangleleft R$ is called a prime ideal if

(1) I is a proper ideal;

(2) $ab \in I \Rightarrow a \in I$ or $b \in I$.

<u>Theorem</u>. I is prime $\Leftrightarrow$ R/I is an integral domain.

- I : maximal $\Rightarrow$ I : prime.
- Suppose R/I is finite; I : prime $\Leftrightarrow$ I : maximal.

Summary

Thursday, March 12, 2020 9:21 PM

<u>Theorem</u>. Suppose D is a PID and $0 \neq a \in D$.

Then $\langle a \rangle$ is maximal $\iff$ a is irreducible.

($\mathbb{Q}[x]$: PID ; $m_\alpha(x)$: irred. ; $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/\langle m_\alpha(x) \rangle$

and the above theorem imply $\mathbb{Q}[\alpha]$ is a field.)

- <u>Theorem</u>. D : PID and $0 \neq I \triangleleft D$. Then

$$I \text{ prime} \iff I \text{ maximal}.$$

- To show an integral domain D is not a PID it is enough to find $a \in D$ s.t.

(1) a is irreducible (2) $\langle a \rangle$ is not prime.

We used the above to show $\mathbb{Z}[\sqrt{-10}]$ is not a PID.

We used $N : \mathbb{Z}[\sqrt{-10}] \to \mathbb{Z}$, $N(a+\sqrt{-10}\, b) := a^2+10b^2$

to show $\sqrt{-10}$ is irreducible. Then we showed

$\langle \sqrt{-10} \rangle$ is not prime;

$$2 \cdot 5 \in \langle \sqrt{-10} \rangle \text{ and } 2 \notin \langle \sqrt{-10} \rangle,\ 5 \notin \langle \sqrt{-10} \rangle.$$

Summary

Thursday, March 12, 2020 9:45 PM

We defined a <u>Unique Factorization Domain</u> (UFD): an integral domain such that

(1) $\forall\, a \in D$ and $a \notin \{0\} \cup D^{\times}$, a can be written as a product of irreducibles (Existence)

(2) If p_i's and q_j's are irreducible and $p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and $p_i = u_i\, q_{\sigma_i}$ for some $u_i \in D^{\times}$ and a permutation σ. (Uniqueness).

<u>Theorem</u>. In a PID the uniqueness part holds.

(Proof of the above theorem was based on induction and the following result:

$p, q_1, \ldots, q_m$: irred. $p \mid q_1 \cdots q_m$ implies $\exists\, i$ and $u \in D^{\times}$ s.t. $p = u\, q_i$.)

<u>Theorem</u>. $F[x]$ is a UFD.

($\mathbb{Z}$ is a UFD.)

Summary

Thursday, March 12, 2020 9:33 PM

Finding a zero in a larger field.

Theorem. Suppose F is a field and $f(x) \in F[x]$ is a monic irreducible polynomial. Then there are E and $\alpha \in E$ s.t.

(1) E is a field and $\exists\ i: F \to E$ an injective ring homomorphism (we say E is a field extension of F.)

(2) $f(\alpha) = 0$ (It is more formal to write $i(f)(\alpha) = 0$ where

$$i(a_0 + a_1 x + \cdots + a_d x^d) = i(a_0) + i(a_1)x + \cdots + i(a_d)x^d.)$$

(3) $E = \{b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1} \mid b_i \in F\}$ where $d = \deg f$.

(4) $c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} = c_0' + c_1'\alpha + \cdots + c_{d-1}'\alpha^{d-1}$, $c_i, c_i' \in F$ $\Rightarrow c_i = c_i'\ \forall i$.

Summary

Thursday, March 12, 2020 9:44 PM

Applying the previous theorem repeatedly we got:

Theorem. Suppose F is a field and $f(x) \in F[x] \setminus \{0\}$.
Then $\exists$ a field E and $\alpha_1, \dots, \alpha_n \in E$ s.t.

$$f(x) = c\,(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

for some $c \in F$.

$\boxed{\text{Finite fields}}$

Theorem. Suppose $f(x) \in \mathbb{Z}_p[x]$ is monic and irreducible, and $\deg f = d$. Then there are E and $\alpha \in E$ s.t.

(1) E is a field, $\mathbb{Z}_p \subseteq E$;

(2) $|E| = p^d$.

(3) $f(\alpha) = 0$.

(4) $f(x) \mid x^{p^d} - x$.

Theorem. Suppose p is prime and d is a positive

Summary

Thursday, March 12, 2020 10:02 PM

integer; then $\exists$ a finite field $\mathbb{F}_{p^d}$ s.t.

$|\mathbb{F}_{p^d}| = p^d$.

Theorem. $x^{p^d} - x = \prod_{\alpha \in \mathbb{F}_{p^d}} (x - \alpha)$.

(We recalled that in a finite group G of order n we have $g^n = 1$ $\forall g \in G$; used this to show $\forall \alpha \in \mathbb{F}_{p^n}$, $\alpha^{p^n} = \alpha$.)