1 Group 1

Def 10.1 群: 封闭, 结合律, 单位元, 逆元

Def 10.2 交换群/阿贝尔群

Lemma 10.4 单位元唯一 $1' = 1'1 = 1$

Lemma 10.5 逆元唯一 $b = 1b = (b'a)b = b'(ab) = b'1 = b'$

THM 10.6 群的等价定义: 封闭, 结合律, 左单位元, 左逆元
| $xx' = exx' = x''x'xx' = x''ex' = x''x' = e \quad xe = xx'x = ex = x$

THM 10.7 群的等价定义: 封闭, 结合律, $ax = y$ 和 $ya = b$ 有解

THM 10.8 **有限**群的等价定义: 封闭, 结合律, 左消去律, 右消去律 10.7 $x \mapsto ax$ 是双射

Lemma 10.9 $(ab)^{-1} = b^{-1}a^{-1}$ $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = bb^{-1} = 1$

Lemma 10.10 $a^{m+n} = a^m a^n$; $a^{mn} = (a^m)^n$

Def 10.11 子群: **非空**, 封闭, 单位元, 逆元; ab^{-1}; 非平凡子群: $H \neq G$; $H \preceq G$, $H \prec G$ $aa^{-1} \quad eb^{-1} \quad a(b^{-1})^{-1}$

Ext 10.11 子群的等价定义: $HH \subseteq H$, $H^{-1} \subseteq H$

Lemma 10.12 $H, K \preceq G \implies H \cap K \preceq G$

Def 10.13 同构: 双射, $f(ab) = f(a)f(b)$

Fact 10.14 $f(e) = e$, $f(a^{-1}) = f(a)^{-1}$

Def 10.15 生成的子群: $\langle A \rangle = \bigcup H_i$; 生成元集

Ext 10.15 $\langle A \rangle = \{x_1 \dots x_n \mid n \in \mathbb{N}, x_i \in A \cup A^{-1}\}$; $\langle a \rangle = \{a^r \mid r \in \mathbb{Z}\}$; $ab = ba \implies \langle a, b \rangle = \{a^m b^n \mid m, n \in \mathbb{Z}\}$

Lemma 10.16 $a \in G \implies \{a^n \mid n \in \mathbb{Z}\} \preceq G$

Def 10.17 循环群: $G = \langle a \rangle$

Ext 10.17 循环群只有两种形状: 无限 $\{\dots, a^{-n}, \dots, a^{-1}, 1, a, \dots, a^m, \dots\}$; 有限 $\{1, a, \dots, a^{n-1}\}$

Ext 10.17 最小的非循环群 K_4:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Def 10.18 元素的阶: 最小正整数 n, $a^n = 1$

Def 10.19 群的阶: 元素个数 $|G|$

Lemma 10.20 -
$\operatorname{ord} g = t, g^m = 1 \implies t \mid m$
$\operatorname{ord} g = t \implies \operatorname{ord} g^s = t/\gcd(t, s), \operatorname{ord} g^s = \operatorname{ord} g^{\gcd(t,s)}$
$\operatorname{ord} g = t, \gcd(t, s) = 1 \implies \operatorname{ord} g^s = t$
$\operatorname{ord} g = \operatorname{ord} g^{-1}$

THM 10.21 循环群的子群也是循环群

THM 10.22 -
若 $|G| = \infty$, 则 G 的生成元只有 a 和 a^{-1}, G 的所有子群 $\{\langle a^d \rangle \mid d = 0, 1, 2, \dots\}$
若 $|G| = n$, 则有 $\phi(n)$ 个生成元 $a^r, \gcd(n, r) = 1$, G 的所有子群 $\{\langle a^d \rangle \mid 0 \leq d \leq n-1, d \mid n\}$

Def 11.4 -
对称群: **非空**集合 M 上所有可逆变换的全体 $T(M)$, 乘法为变换的合成
变换群: 对称群的子群

THM 11.10 $Aut(\mathbb{F})$ 表示数域 $\mathbb{F}$ 所有自同构的全体, 则 $Aut(\mathbb{F})$ 与变换的合成构成群, 称为自同构群

Def 11.14 $\mathbb{F} \subseteq \mathbb{E}$, $\mathbb{E}$ 在 $\mathbb{F}$ 上的对称群: $Aut(\mathbb{E} : \mathbb{F}) = \{\phi \in Aut(\mathbb{E}) \mid \forall x \in \mathbb{F}, \phi(x) = x\}$

Def 11.16 数域 $\mathbb{F}$ 上的 n 元多项式

Def 11.17 $|M| = n$, n 元对称群 S_n: 集合 M 上的变换群

Def 11.18 $\mathbb{F}[x]$ 的 n 元置换群

Def 11.19 多项式 $f(x_1, x_2, \ldots, x_n)$ 的对称群: $S_f = \{\phi_\sigma \in T_n \mid \phi_\sigma(f) = f\}$

Def 11.21 对称多项式: $S_f = T_n$

THM 11.22 Cayley 定理: 任何群都同构于一个变换群 $T : G \to \{T_g : x \to gx \mid g \in G\}$

Def 12.1 排列: **有限**集 S 上的双射

Fact 12.4 $|S_n| = n!$

Fact 12.5 轮换: $(x, \pi(x), \pi(\pi(x)), \ldots)$; 偶轮换; 对换

Fact 12.7 轮换的组合; 不相交循环

Fact 12.8 不相交的轮换满足交换律

THM 12.9 任何置换可以唯一表示为不相交轮换的组合 对元素个数 n 归纳

Fact 12.10 $\sigma = \sigma_1\sigma_2 \ldots \sigma_t$ 是轮换分解, 则 $\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_t))$

Fact 12.11 $a, \ldots, b, c, \ldots, d, k, l$ 互不相同, 则
$(k\ l)(k\ a\ \ldots\ b)(l\ c\ \ldots\ d) = (k\ a\ \ldots\ b\ l\ c\ \ldots\ d)$
$(k\ l)(k\ a\ \ldots\ b\ l\ c\ \ldots\ d) = (k\ a\ \ldots\ b)(k\ c\ \ldots\ d)$

Def 12.12 偶置换: 轮换分解中有偶数个**偶**轮换; 奇置换

THM 12.13 轮换可以分解为对换的合成

Fact 12.14 偶置换可以被分解为偶数个对换; 奇置换可以被分解为奇数个对换

THM 12.15 奇置换分解的对换个数必为奇数; 偶置换分解的对换个数必为偶数

Fact 12.16 两个偶置换的合成为偶置换; 两个奇置换的合称为偶置换; 一奇一偶置换的合称为奇置换

Def 12.17 对称群 S_n: 所有置换; 交错群 A_n: 所有偶置换

Fact 12.18 $|S_n| = n!$; $|A_n| = \dfrac{1}{2}n!, n > 1$

2 Group 2

Def 1.1 左陪集: $gH = \{gh : h \in H\}$; 右陪集

Lemma 1.3 H 是 G 的有限子群, 则 $|gH| = |H|$

Lemma 1.4 $g \in gH$; 若 $b = ah, h \in H$, 则 $aH = bH$; 若 $aH \cap bH \neq \varnothing$, 则 $aH = bH$

Fact 1.5 左陪集和右陪集一样多 双射 $aH \to Ha^{-1}$

Def 1.6 指数 $[G : H]$: 左陪集的个数

THM 1.7 Lagrange 定理: $|G| = |H|\,[G : H]$; 若 G 有限, 则 $|H| \mid |G|$ 有 $[G : H]$ 个大小均为 $|H|$ 不相交的陪集

Cor 1.8 若 $a \in G$, 则 $|\langle a\rangle| \mid |G|$; $a^{|G|} = 1$; 素数阶群都是循环群

THM 1.9 Euler 定理: a, n 互素, $n \geq 2$, 则 $a^{\phi(n)} \equiv 1 \pmod{n}$ $|(\mathbb{Z}_n^*, \cdot)| = \phi(n)$

Cor 1.10 Fermat 小定理: a 是素数, $p \nmid a$, 则 $a^{p-1} \equiv 1 \pmod{p}$

Eg 1.11 RSA
p, q 是素数, $N = pq$, $\phi(N) = (p-1)(q-1)$, $\gcd(e, \phi(N)) = 1$, $d = e^{-1} \pmod{\phi(N)}$, $pk = (N, e)$, $sk = d$
明文 $M \in \mathbb{N}$, 密文 $C \equiv M^e \pmod{N}$, 解密 $M \equiv C^d \pmod{N}$

THM 1.12 $[G : K] = [G : H][H : K]$ $f : \{(a, b) \mid a \text{ 是 } H \text{ 在 } G \text{ 中的陪集首}, b \text{ 是 } K \text{ 在 } H \text{ 中的陪集首}\} \to G/K$ 是双射

THM 1.14 $HK \preceq G \iff HK = KH$, 且此时 HK 由 $H \cup K$ 生成
| $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$, $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, $(HK)(HK) = HKHK = HHKK = HK$

Lemma 1.15 $(aH)(bH) = abH, \forall a, b \in G \iff cHc^{-1} = H, \forall c \in G$
| $cHc^{-1} \subseteq cHc^{-1}H = (cH)(c^{-1}H) = cc^{-1}H = H$, $(aH)(bH) = a(Hb)H = abHH = abH$

Lemma 1.16 $H \trianglelefteq G$ (满足一个): $cHc^{-1} \subseteq H$; $cHc^{-1} = H$; $cH = Hc$; 所有左陪集都是右陪集; 所有右陪集都是左陪集

Def 1.17 商环

Def 1.19 环同构: f(ab) = f(a)f(b)

Lemma 1.20 $f(1) = 1$; $f(a^{-1}) = f^{-1}(a)$

Def 1.21 核 $\ker f = \{a \in G \mid f(a) = 1\}$

Fact 1.22 $\ker f \trianglelefteq G$

Def 1.24 自然同态: $\pi : G \mapsto G/N, a \to aN$; $\ker \pi = N$

Lemma 1.25 f 是单同态当且仅当 $\ker f = \{1\}$

Lemma 1.27 -
若 $M \preceq G$, 则 $f(M) \preceq G'$; 若 $M \trianglelefteq G$ 且 f 是满同态, 则 $f(M) \trianglelefteq G'$
若 $K \preceq G'$, 则 $f^{-1}(K) \preceq G$; 若 $K \trianglelefteq G'$, 则 $f^{-1}(K) \trianglelefteq G$

THM 1.28 同态分解定理: $\ker f = K \supseteq N$**, 则有唯一的同态** $\overline{f} : G/N \mapsto G'$ **使得** $\overline{f} \circ \pi = f$ $\quad \overline{f} : aN \to f(a)$
$\overline{f}$ 是满同态当且仅当 f 是满同态; $\overline{f}$ 是单同态当且仅当 $K = N$

THM 1.29 第一同构定理: $G/\ker f \cong \operatorname{img} f$

Lemma 1.30 $N \trianglelefteq G$, 则: $HN = NH \preceq G$; $N \trianglelefteq HN$; $H \cap N \trianglelefteq H$

THM 1.31 第二同构定理: $H \preceq G$**,** $N \trianglelefteq G$**, 则** $H/(H \cap N) \cong HN/N$ $\quad f : H \to HN/N, h \mapsto hN$

THM 1.32 第三同构定理: $H, N \trianglelefteq G$**,** $N \subseteq H$**, 则** $G/H \cong (G/N)/(H/N)$ $\quad f : G/N \to G/H, aN \mapsto aH$

THM EXT $N \trianglelefteq G$, 则 $\psi : \{H \mid N \preceq H \preceq G\} \to \{H \mid H \preceq G/N\}, H \mapsto H/N$ 是同构
$H_1 \preceq H_2 \iff H_1/N \preceq H2/N$, 且 $[H_2 : H_1] = [H_2/N : H_1/N]$ $\quad aH_1 \to (aN)(H_1/N)$
$H \trianglelefteq G \iff H/N \trianglelefteq G/N$ $\quad \ker(f : a \to (aN)(H/N)) = H$
$H_1 \trianglelefteq H_2 \iff H_1/N \trianglelefteq H_2/N$, 且 $H_2/H_1 \cong (H_2/N)(H_1/N)$

Lemma 2.1 $|\langle a \rangle| = n$, $m \mid n$, 则存在 $H \preceq \langle a \rangle$ 使得 $|H| = m$

Lemma 2.2 $|G| = n$ 是有限交换群, $n = pm$, p 是素数, 则 G 中有 p 阶元素 $\quad$ 对 m 进行归纳

THM 2.3 $|G| = n$ 是有限交换群, $m \mid n$, 则存在 $H \preceq G$ 使得 $|H| = m$ $\quad$ 对 m 进行归纳

Def 3.1 群在集合上的作用: $x \to g \bullet x$ 是双射, $h \bullet (g \bullet x) = (hg) \bullet x$, $1 \bullet x = x$
定义了 G 到 S_X 的同态, $g \bullet x = \Phi(g)(x)$

Def 3.2 中心元: $ax = xa, \forall x \in G$; 群 G 的所有中心元构成 G 的子群

Def 3.3 轨道: $B(x) = \{gx \mid g \in G\}$

Ext 3.3 $y \sim x \iff y = gx$, 则 $\sim$ 是等价关系

Def 3.4 传递: $B(x) = X, \forall x \in X$

Def 3.5 稳定子: $G(x) = \{g \in G \mid gx = x\}$

Ext 3.5 $G(x) \preceq G$; $y = ax$, 则 $G(y) = aG(x)a^{-1}$

THM 3.11 轨道-稳定子定理: $|B(x)| = [G : G(x)]$ $\quad f : gx \mapsto gG(x)$

THM 3.12 $|G| = |C| + \sum_{C(x)} [G : C(x)]$

THM 3.13 $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$

THM 3.14 Burnside 引理: 轨道数量为 $\dfrac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \bullet x = x\}|$

| $\sum_{g \in G} |F(g)| = \sum_{x \in X} |G(x)| = \sum_{B(x)} |B(x)|\,|G(x)| = \sum_{B(x)} |G|$

Def 4.1 p-群: 所有元素的阶都是 p 的幂次; Sylow p-子群: $|P| = p^r, P \preceq G, |G| = p^r m, p \nmid m$

Lemma 4.3 $n = p^r m$, 则 $\binom{n}{p^r} \equiv m \pmod{p}$

THM Sylow1 Sylow 第一定理: G **至少有一个 Sylow** p**-子群; 所有 Sylow-**p **子群都被一个 Sylow** p**-子群包含** G 在 G 的所有子集的集合上的左乘作用

Cor 4.4 $p \mid |G|$, 则 G 有 p 阶元素 $\operatorname{ord}(g) = p^i, g^{p^{i-1}}$

Cor 4.5 G 是 p 群当且仅当 G 的阶是 p 的幂次

THM Sylow2 Sylow 第二定理: 设 n_p **为 Sylow** p**-子群的个数, 则** $n_p \equiv 1 \pmod p$, $n_p \mid m$ P 在所有 Sylow p-子群的集合上的共轭作用

THM Sylow3 Sylow 第三定理: 所有 Sylow p**-子群共轭** p-子群在 P 的左陪集上的左乘作用

Def 4.6 共轭元素类; 中心元 a 的等价类为 a; 共轭关系是等价关系; 共轭子群类

Def 4.7 正规化子: $N(S) = \left\{g \in G \mid gSg^{-1} = S\right\}$; $N(S) \preceq G$; 若 $S \preceq G$, 则 $S \trianglelefteq N(S)$

Lemma 4.8 G 是有限群, $|S|$ 是 G 的共轭元素类, 则存在 $H \preceq G$ 使得 $[G:H] = t$ $xsx^{-1} = ysy^{-1} \iff xN(s) = yN(s)$

THM 4.9 $|G| = n = p^r m$, 则存在 $H \preceq G$ 使得 $|H| = p^r$ 对 n 进行归纳, 分 $C = G$, $p \mid |C|$, $p \nmid |C|$ 讨论

Def 5.1 群的外直积: $\overline{G} = H \times K = \{(h,k) \mid h \in H, k \in K\}$

THM 5.3 $\overline{G}$ 有限当且仅当 H, K 都有限, 且 $\left|\overline{G}\right| = |H|\,|K|$; $\overline{G}$ 是 Abel 群当且仅当 H, K 都为 Abel 群; $H \times K \cong K \times H$

THM 5.4 $\operatorname{ord}((a,b)) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$

THM 5.5 H, K 是循环群, $|H| = m, |K| = n$, 则 $H \times K$ 是循环群当且仅当 $\gcd(m,n) = 1$

Def 5.6 $H, K \trianglelefteq G$, $G = HK$, $H \cap K = \{1\}$, 则记 $G = H \otimes K$

THM 5.7 内直积的等价定义: 每个元素可唯一分解, $hk = kh$

Lemma 5.9 $H \otimes K \cong H \times K$

THM 5.12 $G = H_1 \dots H_n$ 且 $H_i \trianglelefteq G$, 则以下条件等价: G 中任意元素有唯一表示; $H_i \cap \prod\limits_{j \neq i} H_j = \{1\}$; $H_i \cap \prod\limits_{j=1}^{i-1} H_j = \{1\}$

Lemma 6.1 Abel 群 G, $g_1 \dots g_m = 1$, 阶 t_i 两两互素, 则 $g_i = 1, \forall i$ 对 m 归纳

THM 6.2 有限交换群 $|G| = n = p_1^{m_1} \dots p_t^{m_t}$, 则 $G = H_1 \otimes \dots \otimes H_t$, H_i 是 Sylow p_i-群; 上述分解方法唯一

THM 6.3 有限 p-群 G 有 $G = g_1^{\mathbb{Z}} \otimes \dots \otimes g_k^{\mathbb{Z}}$; 上述分解方法唯一

THM 6.4 有限交换群可以唯一分解为阶为素数的幂的循环群的直积

3 Ring 1

Def 1.1 环: 加法交换群, 乘法结合律, 乘法对加法分配律; 有单位元的环; 交换环

Def 1.3 零因子; 单位; 没有零因子的环满足消去律

Def 1.4 整环: 乘法交换律, 有乘法单位元, 无零因子

Def 1.5 除环: 所有非零元有逆元

Def 1.6 域: 交换除环

Fact 1.7 有限整环都是域

Def 1.8 特征: 最小 n 使得 $n1 = 0$, 如果 $n1$ 不可能为 0, 则记特征为 0; 整环的特征是 0 或素数

Lemma 1.10 环的广义分配律: $\sum\limits_{i=1}^{m} a_i \sum\limits_{j=1}^{n} b_j = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} a_i b_j$

Lemma 1.11 交换环上的二项式定理: $(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Def 1.12 子环

THM 1.13 子环的交是子环

Def 1.14 集合生成的子环; 子环的生成元集

THM 1.15 $\langle S\rangle = \bigcap_{S\subseteq A\preceq R} A$

Def 2.1 环同构: $f(a+b)=f(a)+f(b),\ f(ab)=f(a)f(b),\ f(1)=1$

Def 2.3 环同态的核 $\ker f=\{r\in R\mid f(r)=0\}$

Def 2.4 理想: I 是 R 的加法子群, $rI\subseteq I,\forall r\in R,\ Ir\subseteq I,\forall r\in R$; 左理想; 右理想; 非平凡理想

Fact 2.5 $\ker f$ 是理想

Def 2.6 商环: $R/I=\{r+I\mid r\in R\}$

Lemma 2.7 每个非平凡理想都是环同态的核 $\pi: R\mapsto R/I, r\to r+I$

Lemma 2.8 若 R 的理想都是平凡的, 则 $f: R\mapsto S$ 是单环同态

Def 2.9 集合生成的理想; 主理想: 一个元素生成的理想

$(X)=\left\{\sum_{x\in X}x+\sum_{x\in X}xr_i+\sum_{x\in X}r_jx+\sum_{x\in X}r_uxr_v\right\}$; 有 1 环: $(X)=\left\{\sum_{x\in X}r_uxr_v\right\}$; 有 1 交换环: $(X)=\left\{\sum_{r\in R,x\in X}rx\right\}$

Fact 2.10 有 1 交换环中, $\langle a\rangle=\{ra\mid r\in R\}=Ra=aR$

Def 2.11 $I+J$ 也是理想; $I\cap J$ 也是理想

THM 3.1 环同态分解定理: $\ker f\supseteq I$**, 则有唯一的同态** $\overline{f}: R/I\mapsto S$ **使得** $\overline{f}\circ\pi=f$
$\overline{f}$ 是满同态当且仅当 f 是满同态; $\overline{f}$ 是单同态当且仅当 $\ker f=I$

THM 3.2 第一环同构定理: $R/\ker f\cong \operatorname{img} f$

THM 3.3 $S+I\prec R$; I 是 $S+I$ 的理想; $S\cap I$ 是 S 的理想; **第二环同构定理:** $(S+I)/I\cong S/(S\cap I)$

THM 3.4 第三环同构定理: I,J **是** R **的理想,** $J\subseteq I$**, 则** $R/J\cong(R/I)/(J/I)$

THM 3.5 环的一一对应定理: I **是** R **的理想, 则** $\psi:\{S\mid I\preceq S\preceq R\}\to\{S\mid S\preceq R/I\}$ **是同构**

Def EXT 环的外直积

THM CRT 中国剩余定理: $I_1,\dots,I_n$ 是 R 的理想, $I_i+I_j=R,\forall i\neq j$, 则
如果 $a_1=1,a_j=0,\forall j\neq 1$, 则存在 $a\in R,\ a\equiv a_i\pmod{I_i},\forall i$
$\forall a_1,\dots,a_n\in R$, 存在 $a\in R,\ a\equiv a_i\pmod{I_i},\forall i$
$b\equiv a_i\pmod{I_i},\forall i\iff b\equiv a\pmod{I_1\cap\cdots\cap I_n}$
$R/\bigcap I_i\cong R/I_1\times\cdots\times R/I_n$

4 Ring 2

Def 1.1 极大理想: 不被其他真理想包含的真理想

THM 1.2 所有真理想都被一个极大 x 真理想包含; 所有环都有至少 1 个极大理想

THM 1.3 M 是交换环 R 的理想, 则 M 是极大理想当且仅当 R/M 是域

Def 1.4 素理想: 交换环的非平凡理想满足 $ab\in P\Rightarrow a\in P$ or $b\in P,\forall a,b\in R$

THM 1.5 P 是交换环 R 的理想, 则 P 是素理想当且仅当 R/P 是整环

Cor 1.6 $f: R\mapsto S$ 是交换环满同态, 则: 若 S 是域, 则 $\ker f$ 是极大理想; 若 S 是整环, 则 $\ker f$ 是素理想

Cor 1.7 交换环的极大理想都是素理想

Def 2.1 多项式环; R 是交换环, 则 $R[x]$ 是交换环; R 是有 1 环, 则 $R[x]$ 是有 1 环; R 是整环, 则 $R[x]$ 是整环

EXT $f,g\in R[x]$, g 首一, 则 $\exists!q,r\in R[x]$ 使得 $f=qg+r$ 且 $\deg r<\deg g$; 若 R 是域, 则 g 可以为非零多项式

THM 2.2 余式定理: $f(X)=q(X)(X-a)+f(a)$, 且 $f(a)=0\iff X-a\mid f(X)$

THM 2.3 R 是整环, 则非零 n 次多项式 $f\in R[x]$ 最多有 n 个根 对 n 归纳

Def 3.1 单位; 相伴; 不可约元; 素元; $p\neq 0$ 时素元当且仅当 (p) 是素理想; (0) 是任何整环的素理想

Lemma 3.2 素元都不可约

Def 3.3 最大公因数: $d\mid a,\forall A$, $\forall e,e\mid a,\forall A,e\mid d$

Fact 3.4 最大公因数在相伴意义下唯一

Def 3.5 互素: 1 是最大公因数

Def 3.6 最小公倍数

EXT $a \mid b \iff (b) \preceq (a)$

Def 3.7 唯一分解整环: $\forall 0 \neq a \in R$, $a = up_1 \dots p_n$, u 是单位, p_i 不可约, $n \in \mathbb{N}$, 且在无序和相伴意义下唯一

THM 3.8 唯一分解整环中, 不可约元与素元等价

THM EXT (1) 真因子链有限; (2) 非零非单位元可以被分解为有限个不可约元之积; (3) 不可约元都是素元;
(1)(2) $\iff$ UFD $\iff$ (2)(3)

Def 3.10 主理想整环: 任意理想都是主理想

Def 3.11 主理想整环都是唯一分解整环

THM 3.12 主理想整环 $\iff$ 唯一分解整环, 且所有非零素理想都是极大理想
|
对环中元素分解所得不可约元个数的最小值归纳

THM 4.1 A 是主理想整环的非空子集, 则 $d = gcd(A) \iff (d) = (A)$

Cor 4.2 A 是主理想整环的非空集合, 则 $gcd(A)$ 可被 $\sigma r_i a_i$ 表出

Def 4.3 欧几里得整环: 存在 $\Psi : R \setminus \{0\} \mapsto \mathbb{Z}^*$, 使得 $\forall a, b \in R$, $a = bq + r$, 其中 $r = 0$ 或 $\Psi(r) < \Psi(b)$

THM 4.4 欧几里得整环都是主理想整环
考虑理想中 $\Psi(a)$ 最小的 a

Def 5.1 $S \subseteq R$, S 是可乘的: $0 \notin S, 1 \in S, ab \in S, \forall a, b \in S$

Def 5.2 定义 $\frac{a}{b}$ 为 (a, b) 的等价关系 $\exists s \in S, s(ad - bc) = 0$ 的等价类; 这样的等价类的集合为分数环

THM 5.3 若 R 是整环, 则 $S^{-1}R$ 也是; 若 R 是整环且 $S = R \setminus \{0\}$, 则 S^{-1} 是域

Fact 5.4 整环的商域是包含它的最小域

Def 6.1 不可约多项式

5 Field

THM 2.1 若 R 有单位元 e, 则 $\phi : \mathbb{Z} \mapsto R, m \to me$ 是环同态
若 $\operatorname{Char} R = 0$, 则 R 包含与 $\mathbb{Z}$ 同构的子环; 若 $\operatorname{Char} R = n$, 则 R 包含与 $\mathbb{Z}_n$ 同构的子环

Lemma 2.2 域同态都是单同态

Def 2.3 若 $\mathbb{F}$ 没有真子域, 则 $\mathbb{F}$ 是素域

THM 2.4 若 $\operatorname{Char} \mathbb{F} = 0$, 则 $\mathbb{F}$ 包含与 $\mathbb{Q}$ 的素子域; 若 $\operatorname{Char} \mathbb{F} = p$ 是素数, 则 $\mathbb{F}$ 包含一个与 $\mathbb{Z}_p$ 同构的素子域

EXT $\mathbb{F}[x]$ 是欧几里得整环

Def 3.1 域的扩张 $\mathbb{F} \leq \mathbb{E}$: $\mathbb{F} \subseteq \mathbb{E}$

Fact 3.2 $\mathbb{F} \leq \mathbb{E}$, 则 $\mathbb{E}$ 是 $\mathbb{F}$ 的向量空间, 其维数称为扩张的次数, 即为 $[\mathbb{E} : \mathbb{F}]$

THM 3.4 $f(x) \in \mathbb{F}[x]$, $\deg(f) \geq 1$, **则存在扩张** $\mathbb{R}/\mathbb{F}$ **和** $\alpha \in \mathbb{E}$ **使得** $f(\alpha) = 0$

THM 3.5 $f, g \in \mathbb{F}[x]$, f, g 互素当且仅当任何扩域内 f, g 没有公共根

Cor 3.6 f, g 是 $\mathbb{F}$ 上的不同不可约首一多项式, 则在任何扩域内 f, g 没有公共根

Def 4.2 $\mathbb{F} \leq \mathbb{E}$, $a \in \mathbb{E}$ 称为 $\mathbb{F}$ 上的代数元: 存在非常值多项式 $f \in \mathbb{F}[x]$ 使得 $f(\alpha) = 0$
不是代数元的称为超越元; 所有元素都是代数元的扩张称为代数扩张

Def 5.0 $\alpha \in \mathbb{E}$ 是 $\mathbb{F}$ 上的代数元, 设 $I = \{g \in \mathbb{F}[x] \mid g(\alpha) = 0\}$, 则 I 是 $\mathbb{F}[X]$ 的理想, 因此也是主理想, 即 I 是某个首一多项式 $m(X) \in \mathbb{F}[X]$ 的所有倍数, $m(X)$ 唯一, 称为 α 在 $\mathbb{F}$ 上的极小多项式, 写作 $\min(\alpha, \mathbb{F})$
$g \in \mathbb{F}[X]$, 则 $g(\alpha) = 0 \iff m(X) \mid g(X)$
$m(X)$ 是满足 $g(\alpha) = 0$ 的多项式中次数最低的那一个
$m(X)$ 是满足 $g(\alpha) = 0$ 的唯一的首一不可约多项式

Def 5.1 $\alpha \in \mathbb{E}$ 是 $\mathbb{F}$ 上的代数元, 其最小多项式 $m(X)$ 的次数为 n, 则 $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$
$\mathbb{F}[\alpha]$ 的一组基是 $1, a, \ldots, a^{n-1}$, 且 $[\mathbb{F}(\alpha) : \mathbb{F}] = n$

Lemma 5.2 $\mathbb{F} \leq K \leq \mathbb{E}$, α_i 构成 $\mathbb{E}$ 对于 K 的一组基, β_j 构成 K 对于 $\mathbb{F}$ 的一组基, 则 $\alpha_i\beta_j$ 构成 $\mathbb{E}$ 对于 $\mathbb{F}$ 的一组基

Cor 5.3 $\mathbb{F} \leq K \leq \mathbb{E}$, 则 $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : K][K : \mathbb{F}]$

THM 5.4 $\mathbb{E}/\mathbb{F}$ 是有限扩张, 则 $\mathbb{E}/\mathbb{F}$ 是代数扩张

THM 6.1 $\mathbb{F} \leq K$, $S_1 \subset K, S_2 \subset K$, 则 $\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$

Def 6.2 $\mathbb{F} \leq \mathbb{E}$, $f \in \mathbb{F}[X]$, f 在 $\mathbb{E}$ 上分裂: $f = \lambda(X - \alpha_1)\ldots(X - \alpha_k), \alpha_i \in \mathbb{E}, \lambda \in \mathbb{F}$
$\mathbb{F} \leq K$, $f \in \mathbb{F}[X]$, K 是 f 关于 $\mathbb{F}$ 的分裂域: f 在 K 上分裂, 不在 K 包含 $\mathbb{F}$ 的真子域上分裂

THM 6.3 $f \in \mathbb{F}[X]$, $\deg f = n$, 存在 f 的分裂域 K 使得 $[K : \mathbb{F}] \leq n!$

THM 6.4 $f(x) = b(x - \alpha_1)\ldots(x - \alpha_n) \neq 0$ 在 $\mathbb{E}$ 上分裂当且仅当 $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_m)$

THM 6.5 α, β 是不可约多项式 $f \in \mathbb{F}[X]$ 在扩域 E 上的根, 则 $\mathbb{F}(\alpha) \cong \mathbb{F}(\beta)$ 且其中 α 映射为 β 且在 $\mathbb{F}$ 范围内为自身映射

Lemma 6.6 $p(x) \in \mathbb{F}[x]$ 不可约, α 是其在扩域 $\mathbb{E}$ 上的根, 设 $\phi : \mathbb{F} \mapsto \mathbb{F}'$ 是域同构, α' 是 $\phi(p(x))$ 在扩域 E' 上的根, 则存在同构映射 $\mathbb{F}(\alpha) \mapsto \mathbb{F}'(\alpha')$, 在 $\mathbb{F}$ 的范围内即为 ϕ

Def 6.7 $\mathbb{F} \leq \mathbb{E}, \mathbb{F} \leq \mathbb{E}'$, i 是 $\mathbb{E}$ 到 $\mathbb{E}'$ 的自同构, 如果 $i(a) = a$, 则称 i 为 $\mathbb{F}$-同构

THM 6.8 扩域同构定理: $\mathbb{F} \cong \mathbb{F}'$, 同构映射 i 将 $f \in \mathbb{F}[X]$ 映射到 $f' \in \mathbb{F}'[X]$, K 是 f 的分裂域, K' 是 f' 的分裂域, 则 i 可以被扩展为 K 到 K' 的同构

EXT $f(x)$ 的分裂域在 $\mathbb{F}$-同构意义下唯一

Def 6.10 Pythagoras 扩域: $\mathbb{F} \subseteq K \leq \mathbb{R}$, $K = \mathbb{F}(\sqrt{b_1})\ldots(\sqrt{b_m}), b_i > 0, b_1 \in \mathbb{F}, b_i \in \mathbb{F}(\sqrt{b_1})\ldots(\sqrt{b_{i-1}})$

THM 6.11 已知 $1, a_1, \ldots, a_n \in \mathbb{R}$, 尺规可以且仅可以作出 $\mathbb{Q}(a_1, \ldots, a_n)$ 的任意 Pythagoras 扩域中的数

THM 6.12 $\mathbb{E}$ 是 $\mathbb{F}$ 的 Pythagoras 扩域, 则 $[\mathbb{E} : \mathbb{F}] = 2^n$