抽象代数习题整理与解答

Abstract Algebra: Exercises and Solutions

Artin Algebra 作业题: 群论, 环论, 域论与 Galois 理论, 模论

RongYu

抽象代数系列讲义

2026.9.19

Contents

1 第一次作业 2

2 第二次作业 19

3 第三次作业 39

4 第四次作业 47

5 第五次作业 62

6 第六次作业 77

7 第七次作业 87

1

第一次作业

习题 2.3

Let x, y, z, and w be elements of a group G. (a) Solve for y, given that $xyz^{-1}w = 1$. (b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

解答

题目翻译: 设 x, y, z, w 是群 G 的元素. (a) 在等式 $xyz^{-1}w = 1$ 中解出 y. (b) 假设 $xyz = 1$. 能否推出 $yzx = 1$? 能否推出 $yxz = 1$?

解答: (a) 对 $xyz^{-1}w = 1$ 两边左乘 x^{-1}, 得 $yz^{-1}w = x^{-1}$; 两边右乘 w^{-1}, 得 $yz^{-1} = x^{-1}w^{-1}$; 两边右乘 z, 得

$$y = x^{-1}w^{-1}z.$$

(b) 由 $xyz = 1$ 两边左乘 x^{-1}, 得 $yz = x^{-1}$. 于是

$$yzx = (yz)x = x^{-1}x = 1.$$

故 $yzx = 1$ 一定成立.

$yxz = 1$ 不一定成立. 反例: 在 S_3 中取 $x = (12)$, $y = (23)$, $z = (132)$. 则 $xyz = (12)(23)(132) = 1$, 但 $yxz = (23)(12)(132) = (123) \neq 1$. 一般地, $xyz = 1$ 等价于 $z = (xy)^{-1} = y^{-1}x^{-1}$, 此时 $yxz = yxy^{-1}x^{-1}$, 它等于 1 当且仅当 $xy = yx$, 即 x 与 y 交换, 而 S_3 中 x, y 不交换.

习题 2.5

In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity in G. Show that if H has an identity at all, then it is the identity in G. Show that the analogous statement is true for inverses.

解答

题目翻译: 在子群的定义中, 要求 H 中的单位元就是 G 的单位元. 也许可以只要求 H 有一个单位元, 而不必要求它与 G 的单位元相同. 证明: 若 H 确有单位元, 则它就是 G 的单位元. 再证明关于逆元的相应结论.

解答: 设 e 是 H 中关于 G 的乘法运算的单位元, 即对一切 $h \in H$ 有 $eh = he = h$. 由于 $e \in H \subseteq G$ 且 $ee = e$ (取 $h = e$), 在 G 中等式 $ee = e$ 两边右乘 e^{-1}, 得 $e = 1$, 其中

1 是 G 的单位元. 故 H 的单位元必等于 G 的单位元.
关于逆元: 设 $h \in H$, 且 $h' \in H$ 满足 $h'h = hh' = e$. 由上一步 $e = 1$, 故 h' 也是 h 在 G 中的逆元. 群中逆元唯一, 所以 $h' = h^{-1}$. 即 H 中元素 h 在 H 内的逆元就是它在 G 中的逆元.

习题 M.4

A semigroup S is a set with an associative law of composition and with an identity. Elements are not required to have inverses, and the Cancellation Law need not hold. A semigroup S is said to be generated by an element s if the set $\{1, s, s^2, \ldots\}$ of nonnegative powers of s is equal to S. Classify semigroups that are generated by one element.

解答

题目翻译: 半群 S 是一个带有结合律的合成法则并且含单位元的集合. 不要求元素有逆元, 消去律也不必成立. 若非负次幂的集合 $\{1, s, s^2, \ldots\}$ 恰等于 S, 则称半群 S 由元素 s 生成. 对由单个元素生成的半群进行分类.
解答: 设 S 由 s 生成, 即 $S = \{s^n : n \geq 0\}$ (约定 $s^0 = 1$). 分两种情形.
情形一: 各 s^n $(n \geq 0)$ 两两不同. 此时映射 $n \mapsto s^n$ 给出 $(\mathbb{N}_0, +)$ 到 $(S, \cdot)$ 的双射, 且 $s^{m+n} = s^m s^n$, 故它是同构. 这里 $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ 是非负整数加法幺半群. 此时 $S \cong (\mathbb{N}_0, +)$.
情形二: 存在 $i < j$ 使 $s^i = s^j$. 设 m 是使 $s^m = s^{m+p}$ (对某个 $p \geq 1$) 成立的最小非负整数, p 取使该式成立的最小正整数. 则 $S = \{1, s, \ldots, s^{m+p-1}\}$, 共 $m + p$ 个元素. 其中集合

$$\{s^m, s^{m+1}, \ldots, s^{m+p-1}\}$$

对乘法封闭, 构成一个 p 阶循环群, 其单位元是 s^r, 其中 r 是区间 $[m, m + p - 1]$ 中唯一的 p 的倍数; 而前 m 个元素 $1, s, \ldots, s^{m-1}$ 不在这个群中, 称为该半群的尾 (tail).
特别地, 若 $m = 0$, 则 $s^p = 1$, $S = \{1, s, \ldots, s^{p-1}\}$ 本身是一个 p 阶循环群, 同构于 $\mathbb{Z}/p\mathbb{Z}$; 若 $m > 0$, 则 S 不是群 (尾中的元素没有逆元).
因此, 单元素生成的半群只有两类: 无限情形同构于非负整数加法幺半群 $(\mathbb{N}_0, +)$; 有限情形由一个可空的尾加上一个循环群组成.

习题 M.5

Let S be a finite semigroup (see Exercise M.4) in which the Cancellation Law holds. Prove that S is a group.

解答

题目翻译: 设 S 是满足消去律的有限半群 (见习题 M.4). 证明 S 是群.
解答: 按习题 M.4 的约定, 半群 S 含单位元 1. 只需证明 S 中每个元素都有逆元.
对任意 $a \in S$, 考虑左乘映射 $L_a : S \to S$, $x \mapsto ax$. 由左消去律, 若 $L_a(x) = L_a(y)$, 则 $ax = ay$, 从而 $x = y$, 故 L_a 是单射. 因 S 有限, 单射必为双射, 故存在 $x \in S$ 使 $ax = 1$, 即 a 有左逆元.
同理, 右乘映射 $R_a : S \to S$, $x \mapsto xa$, 也是双射, 故存在 $y \in S$ 使 $ya = 1$, 即 a 有右逆元. 于是

$$y = y \cdot 1 = y(ax) = (ya)x = 1 \cdot x = x,$$

故 $x = y$, 且 $ax = xa = 1$. 所以 x 是 a 的 (双边) 逆元.
由于 a 任意, S 中每个元素都可逆, 连同结合律与单位元, S 是群.

习题 4.10

Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian?

解答

题目翻译: 举例说明: 一个群中两个有限阶元素的乘积不一定具有有限阶. 若群是交换的, 情形如何?
解答: 考虑实直线上的仿射等距变换群. 令

$$f(x) = -x, \qquad g(x) = -x + 1.$$

f 是关于原点的反射, g 是关于点 $1/2$ 的反射, 二者都满足 $f^2 = g^2 = 1$, 故 f, g 都是 2 阶元. 但它们的复合是平移:

$$(fg)(x) = f(g(x)) = -(-x + 1) = x - 1,$$

其 n 次复合为 $x - n$, 永不等于恒等映射, 故 fg 是无限阶元. 这就是所需的例子.
若群 G 交换, 设 $a^m = 1$, $b^n = 1$. 则由交换性,

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1.$$

故 ab 是有限阶元, 且其阶整除 mn. 所以在交换群里, 有限阶元素的乘积仍为有限阶.

习题 5.1

Let $\phi : G \to G'$ be a surjective homomorphism. Prove that if G is cyclic, then G' is cyclic, and if G is abelian, then G' is abelian.

解答

题目翻译: 设 $\phi : G \to G'$ 是满同态. 证明: 若 G 是循环群, 则 G' 是循环群; 若 G 是交换群, 则 G' 是交换群.

解答: 若 $G = \langle g \rangle$ 由 g 生成, 则 G' 中任一元素形如 $\phi(g^k) = \phi(g)^k$ $(k \in \mathbb{Z})$. 故 $G' = \langle \phi(g) \rangle$ 是循环群.

若 G 交换, 对任意 $a', b' \in G'$, 因 ϕ 满, 存在 $a, b \in G$ 使 $\phi(a) = a'$, $\phi(b) = b'$. 则

$$a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'.$$

故 G' 交换.

习题 5.5

Prove that the $n \times n$ matrices that have the block form $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, with $A \in \mathrm{GL}_r(R)$ and $D \in \mathrm{GL}_{n-r}(R)$, form a subgroup H of $\mathrm{GL}_n(R)$, and that the map $H \to \mathrm{GL}_r(R)$ that sends $M \mapsto A$ is a homomorphism. What is its kernel?

解答

题目翻译: 证明具有分块形式 $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ (其中 $A \in \mathrm{GL}_r(R)$, $D \in \mathrm{GL}_{n-r}(R)$) 的 $n \times n$ 矩阵构成 $\mathrm{GL}_n(R)$ 的子群 H, 并证明把 M 映到 A 的映射 $H \to \mathrm{GL}_r(R)$ 是同态. 它的核是什么?

解答: 先证 H 是子群. 单位元 $I_n = \begin{bmatrix} I_r & 0 \\ 0 & I_{n-r} \end{bmatrix} \in H$. 若 $M_1 = \begin{bmatrix} A_1 & B_1 \\ 0 & D_1 \end{bmatrix}$, $M_2 = \begin{bmatrix} A_2 & B_2 \\ 0 & D_2 \end{bmatrix} \in H$, 则

$$M_1 M_2 = \begin{bmatrix} A_1A_2 & A_1B_2 + B_1D_2 \\ 0 & D_1D_2 \end{bmatrix}.$$

由 $A_1A_2 \in \mathrm{GL}_r(R)$, $D_1D_2 \in \mathrm{GL}_{n-r}(R)$ 知 $M_1M_2 \in H$. 又

$$M^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix},$$

仍具有同一分块形式, 故 $M^{-1} \in H$. 因此 H 是 $\mathrm{GL}_n(R)$ 的子群.

记 $\pi(M)=A$. 由上面的乘法公式,

$$\pi(M_1M_2)=A_1A_2=\pi(M_1)\pi(M_2),$$

故 π 是同态. 它显然满: 对任意 $A\in \mathrm{GL}_r(R)$, 取 $M=\begin{bmatrix}A & 0\\ 0 & I_{n-r}\end{bmatrix}\in H$ 即得.

π 的核为

$$\begin{aligned}\ker\pi&=\left\{M=\begin{bmatrix}A & B\\ 0 & D\end{bmatrix}\in H: A=I_r\right\}\\ &=\left\{\begin{bmatrix}I_r & B\\ 0 & D\end{bmatrix}: D\in \mathrm{GL}_{n-r}(R),\ B \text{ 为任意} r\times(n-r) \text{ 实矩阵}\right\},\end{aligned}$$

即左上角为单位阵的那些分块上三角矩阵.

习题 5.6

Determine the center of $\mathrm{GL}_n(R)$. Hint: You are asked to determine the invertible matrices A that commute with every invertible matrix B. Do not test with a general matrix B. Test with elementary matrices.

解答

题目翻译: 确定 $\mathrm{GL}_n(R)$ 的中心. 提示: 要求确定与每个可逆矩阵 B 都可交换的可逆矩阵 A. 不要用一般的矩阵 B 检验, 用初等矩阵检验.

解答: 中心为

$$Z(\mathrm{GL}_n(R))=\{\lambda I_n:\lambda\in\mathbb{R}^\times\}.$$

显然每个非零标量矩阵 λI_n 与一切矩阵可交换, 故属于中心. 下面证中心中的矩阵必为标量矩阵.

设 $A=(a_{ij})\in Z(\mathrm{GL}_n(R))$. 对 $i\neq j$, 令 E_{ij} 为 (i,j) 位置为 1, 其余位置为 0 的初等矩阵, 则 $AE_{ij}=E_{ij}A$. 左端 AE_{ij} 的第 j 列为 A 的第 i 列, 其余列全为 0; 右端 $E_{ij}A$ 的第 i 行为 A 的第 j 行, 其余行全为 0.

比较 (k,j) 位置 $(k\neq i)$, 得 $a_{ki}=0$; 比较 (i,j) 位置, 得 $a_{ii}=a_{jj}$. 由于 i,j 任意, A 的所有非对角元为 0, 且所有对角元相等. 故 $A=\lambda I_n$. 又 A 可逆, $\lambda\neq 0$.

于是 $Z(\mathrm{GL}_n(R))=\{\lambda I_n:\lambda\in\mathbb{R}^\times\}$. (当 $n=1$ 时, $\mathrm{GL}_1(R)=\mathbb{R}^\times$ 是交换群, 中心为其自身, 结论一致.)

习题 6.1

Let G' be the group of real matrices of the form $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?

解答

题目翻译: 设 G' 是形如 $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ 的实矩阵组成的群. 把 x 映到该矩阵的映射 $\mathbb{R}^+ \to G'$ 是否是同构?

解答: 这里 $\mathbb{R}^+$ 表示实数的加法群 $(\mathbb{R}, +)$, 而

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix},$$

故 G' 在矩阵乘法下成群. 定义 $f : (\mathbb{R}, +) \to G'$, $x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. 由上式,

$$f(x+y) = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = f(x)f(y),$$

故 f 是同态. 又 f 显然单射 (由 $f(x) = f(y)$ 得 $x = y$), 且每个 $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \in G'$ 都等于 $f(t)$, 故 f 满射. 所以 f 是双射同态, 即同构. 答案为是.

习题 6.2

Describe all homomorphisms $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective, and which are isomorphisms.

解答

题目翻译: 描述所有同态 $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$. 判断其中哪些是单射, 哪些是满射, 哪些是同构.

解答: 这里 $\mathbb{Z}^+$ 表示整数加法群 $(\mathbb{Z}, +)$. 由于 $\mathbb{Z}$ 由 1 生成, 同态 ϕ 完全由 $\phi(1)$ 决定: 对任意 $n \in \mathbb{Z}$,

$$\phi(n) = \phi(n \cdot 1) = n\,\phi(1).$$

记 $k = \phi(1) \in \mathbb{Z}$, 则 $\phi(n) = kn$. 反之, 对任意 $k \in \mathbb{Z}$, 映射 $\phi_k : n \mapsto kn$ 显然是同态.

故

$$\mathrm{Hom}(\mathbb{Z}^+,\mathbb{Z}^+)=\{\phi_k : k\in\mathbb{Z}\}.$$

单射性: ϕ_k 单 $\iff \ker\phi_k=\{0\} \iff k\neq 0$ (因为 $\phi_k(n)=0$ 对一切 n 成立当且仅当 $k=0$).
满射性: $\phi_k(\mathbb{Z})=k\mathbb{Z}$, 而 $k\mathbb{Z}=\mathbb{Z}$ 当且仅当 $k=\pm1$.
同构: 既单又满, 故 $k=\pm1$. 即 $\phi_1(n)=n$ 与 $\phi_{-1}(n)=-n$ 是仅有的两个自同构.

习题 6.3

Show that the functions $f=1/x$, $g=(x-1)/x$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group S_3.

解答

题目翻译: 证明函数 $f=1/x$ 与 $g=(x-1)/x$ 以函数复合为合成法则, 生成一个与对称群 S_3 同构的函数群.
解答: 记 $f(x)=1/x$, $g(x)=(x-1)/x$, 复合按从右到左进行. 直接计算各函数的复合:

$$f^2(x)=\frac{1}{1/x}=x,\quad \text{故}f^2=1,\ f\text{ 的阶为2;}$$

$$g^2(x)=\frac{(x-1)/x-1}{(x-1)/x}=-\frac{1}{x-1},\qquad g^3(x)=x,$$

故 $g^3=1$, g 的阶为 3. 又

$$(fg)(x)=\frac{1}{(x-1)/x}=\frac{x}{x-1},\qquad (fg)^2(x)=x,$$

故 $(fg)^2=1$, fg 的阶为 2.
于是 $\langle f,g\rangle$ 含有元素 1, f, g, g^2, fg, fg^2, 它们分别是函数 x, $1/x$, $(x-1)/x$, $1/(1-x)$, $x/(x-1)$, $1-x$, 两两不同, 故 $|\langle f,g\rangle|=6$. 又 $fg(x)=x/(x-1)\neq 1-x=gf(x)$, 故该群非交换. 6 阶群在同构意义下只有循环群 $\mathbb{Z}/6\mathbb{Z}$ 与非交换的 S_3 两种, 本例非交换, 因此 $\langle f,g\rangle\cong S_3$.

习题 8.4

Does a group of order 35 contain an element of order 5? of order 7?

解答

题目翻译: 35 阶群是否含有 5 阶元素? 是否含有 7 阶元素?
解答: 两个答案都是肯定的. 由 Lagrange 定理, 任一非单位元的阶整除 $35=5\times7$, 故

只能是 5, 7 或 35.
先证必含 5 阶元素. 反设不含 5 阶元素. 若存在 35 阶元 g, 则 g^7 的阶为 5, 矛盾. 故所有非单位元的阶均为 7. 每个 7 阶元生成一个 7 阶循环子群; 两个不同的 7 阶子群只交于 $\{1\}$, 因为它们的交是子群, 阶整除 7, 真子群只能为 1. 于是 34 个非单位元被划分为若干互不相交的 6 元组, 34 应是 6 的倍数, 矛盾. 所以 G 含 5 阶元素.
同理证必含 7 阶元素: 反设不含 7 阶元素. 若存在 35 阶元 g, 则 g^5 的阶为 7, 矛盾. 故所有非单位元的阶均为 5. 同样地, 两个不同的 5 阶子群只交于 $\{1\}$, 非单位元被划分为 4 元组, 而 34 不是 4 的倍数, 矛盾. 所以 G 含 7 阶元素.

习题 8.8

Let G be a group of order 25. Prove that G has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.

解答

题目翻译: 设 G 是 25 阶群. 证明 G 至少有一个 5 阶子群; 并且若 G 只有一个 5 阶子群, 则 G 是循环群.
解答: 取非单位元 $x \in G$. 由 Lagrange 定理, $|x|$ 整除 25 且 $|x| \neq 1$, 故 $|x| = 5$ 或 25. 若 $|x| = 5$, 则 $\langle x \rangle$ 是 5 阶子群; 若 $|x| = 25$, 则 $\langle x \rangle = G$, 而 $\langle x^5 \rangle$ 是 5 阶子群. 故 G 恒有 5 阶子群.
设 H 是 G 唯一的 5 阶子群. 取 $g \in G \setminus H$ (存在, 因为 $|G| = 25 > 5$). 则 $|g|$ 整除 25, 故 $|g| = 5$ 或 25. 若 $|g| = 5$, 则 $\langle g \rangle$ 是 5 阶子群, 由唯一性 $\langle g \rangle = H$, 与 $g \notin H$ 矛盾. 故 $|g| = 25$, 于是 $\langle g \rangle = G$, G 是循环群.

习题 8.12

Let S be a subset of a group G that contains the identity element 1, and such that the left cosets aS, with $a \in G$, partition G. Prove that S is a subgroup of G.

解答

题目翻译: 设 S 是群 G 的一个含单位元 1 的子集, 并且左陪集 aS ($a \in G$) 构成 G 的一个划分. 证明 S 是 G 的子群.
解答: 对任意 $a \in S$: 因 $1 \in S$, 有 $a = a \cdot 1 \in aS$; 又 $a \in S = 1 \cdot S$. 由于 $\{aS\}$ 是 G 的划分, 含 a 的陪集唯一, 故 $aS = S$.
于是对任意 $a, b \in S$, $ab \in aS = S$, 即 S 对乘法封闭. 又 $1 \in S = aS$, 故存在 $s \in S$ 使 $1 = as$, 从而 $s = a^{-1} \in S$, 即 S 含每个元素的逆元. 连同 $1 \in S$, 由子群判定准则, S 是 G 的子群.

习题 10.4

With the notation of the Correspondence Theorem, let H and H' be corresponding subgroups. Prove that $[G : H] = [G' : H']$.

解答

题目翻译: 采用对应定理的记号, 设 H 与 H' 是互相对应的子群. 证明 $[G : H] = [G' : H']$.

解答: 设 $\phi : G \to G'$ 是核为 N 的满同态. 对应定理说: 映射 $H \mapsto H' = \phi(H)$ 给出 G 中含 N 的子群与 G' 的子群之间的一一对应, 故这里 $H \supseteq N$ 且 $H' = \phi(H)$.
由第三同构定理,

$$G/H \cong (G/N)/(H/N).$$

又 ϕ 诱导同构 $\bar{\phi} : G/N \to G'$, $\bar{\phi}(gN) = \phi(g)$, 它把 H/N 映到 H', 故

$$(G/N)/(H/N) \cong G'/H'.$$

于是 $G/H \cong G'/H'$, 两边陪集个数相等:

$$[G : H] = [G' : H'].$$

(直观上, 由 $N \subseteq H$ 知 H 在 G 中的陪集与 H/N 在 G/N 中的陪集一一对应, 指数相等; 再通过 $G/N \cong G'$ 把指数转移到 G'.)

习题 11.4

In each of the following cases, determine whether or not G is isomorphic to the product group $H \times K$. (a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{\text{positive real numbers}\}$. (b) $G = \{\text{invertible upper triangular } 2 \times 2 \text{ matrices}\}$, $H = \{\text{invertible diagonal matrices}\}$, $K = \{\text{upper triangular matrices with diagonal entries } 1\}$. (c) $G = \mathbb{C}^\times$, $H = \{\text{unit circle}\}$, $K = \{\text{positive real numbers}\}$.

解答

题目翻译: 在下列各情形中, 判断 G 是否同构于积群 $H \times K$. (a) $G = \mathbb{R}^\times$ (非零实数乘法群), $H = \{\pm 1\}$, $K =$ 正实数乘法群. (b) $G =$ 可逆上三角 2×2 矩阵群, $H =$ 可逆对角矩阵群, $K =$ 对角元全为 1 的上三角矩阵群. (c) $G = \mathbb{C}^\times$ (非零复数乘法群), $H =$ 单位圆周, $K =$ 正实数乘法群.

解答: (a) 是. 映射 $(\varepsilon, t) \mapsto \varepsilon t$ ($\varepsilon = \pm 1$, $t > 0$) 是 $H \times K \to G$ 的同态:

$$(\varepsilon_1\varepsilon_2,\ t_1t_2) \mapsto \varepsilon_1\varepsilon_2\, t_1t_2 = (\varepsilon_1 t_1)(\varepsilon_2 t_2).$$

它也是双射: 每个非零实数 r 唯一表为 $r = \operatorname{sgn}(r) \cdot |r|$. 故 $\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$.

(b) 否. $H \cong \mathbb{R}^\times \times \mathbb{R}^\times$ 与 $K \cong (\mathbb{R}, +)$ 都是交换群, 故 $H \times K$ 交换. 但 G (可逆上三角矩阵群) 非交换: 例如对角阵 $\mathrm{diag}(2,1)$ 与单位上三角阵 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ 不交换. 同构保持交换性, 故 $G \ncong H \times K$.
(c) 是. 映射 $(u,t) \mapsto ut$ ($|u| = 1, t > 0$) 是同态: $(u_1u_2,\ t_1t_2) \mapsto u_1u_2\,t_1t_2 = (u_1t_1)(u_2t_2)$. 它双射, 逆映射为 $z \mapsto (z/|z|,\ |z|)$. 故 $\mathbb{C}^\times \cong S^1 \times \mathbb{R}_{>0}$.

习题 11.9

Let H and K be subgroups of a group G. Prove that the product set HK is a subgroup of G if and only if $HK = KH$.

解答

题目翻译: 设 H 与 K 是群 G 的子群. 证明: 积集 HK 是 G 的子群当且仅当 $HK = KH$.
解答: ($\Leftarrow$) 设 $HK = KH$. 显然 $1 = 1 \cdot 1 \in HK$. 若 $h_1k_1,\ h_2k_2 \in HK$, 则

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2.$$

因 $k_1h_2 \in KH = HK$, 存在 $h' \in H,\ k' \in K$ 使 $k_1h_2 = h'k'$, 故乘积 $= h_1h'k'k_2 \in HK$, 封闭性得证. 又

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

所以 HK 是子群.
($\Rightarrow$) 设 HK 是子群. 对 $hk \in HK$, 因 HK 是子群, 有 $(hk)^{-1} = k^{-1}h^{-1} \in HK$, 故存在 $h' \in H,\ k' \in K$ 使 $k^{-1}h^{-1} = h'k'$, 于是

$$hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH.$$

故 $HK \subseteq KH$. 反之, 对 $kh \in KH$, 有 $h^{-1}k^{-1} \in HK$; 因 HK 是子群, 其逆元 kh 也在 HK 中, 故 $KH \subseteq HK$. 综上 $HK = KH$.

习题 2.6

Let G be a group. Define an opposite group G° with law of composition $a * b$ as follows: The underlying set is the same as G, but the law of composition is $a * b = ba$. Prove that G° is a group.

解答

题目翻译: 设 G 是群. 定义反群 G°, 其合成法则 $a*b$ 规定如下: 底层集合与 G 相同, 但合成法则为 $a*b=ba$. 证明 G° 是群.
解答: 封闭性: 对 $a,b\in G^\circ$, $a*b=ba\in G$, 故 $a*b\in G^\circ$.
结合律:

$$(a*b)*c=(ba)*c=c(ba)=cba,\qquad a*(b*c)=a*(cb)=(cb)a=cba.$$

故 $(a*b)*c=a*(b*c)$.
单位元: G 的单位元 1 也是 G° 的单位元: $1*a=a\cdot 1=a$, $a*1=1a=a$.
逆元: 对 $a\in G^\circ$, a 在 G 中的逆元 a^{-1} 满足

$$a*a^{-1}=a^{-1}a=1,\qquad a^{-1}*a=aa^{-1}=1,$$

故 a^{-1} 是 a 在 G° 中的逆元.
所以 G° 是群. 附带指出, 映射 $g\mapsto g^{-1}$ 是 G 到 G° 的同构, 故 $G^\circ\cong G$.

习题 4.5

Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents, and use the description of the subgroups of $\mathbb{Z}^+$.

解答

题目翻译: 证明循环群的每个子群都是循环群. 用指数来做, 并利用 $\mathbb{Z}^+$ 的子群的描述.
解答: 设 $G=\langle g\rangle$ 是循环群, $H\le G$. 若 $H=\{1\}$, 则 H 是循环群. 否则, H 含某个 $g^k\neq 1$ ($k\neq 0$), 则 $g^{|k|}\in H$ (因为 $g^{-k}=(g^k)^{-1}\in H$), 故集合 $\{n\in\mathbb{Z}_{>0}:g^n\in H\}$ 非空, 由良序原理取最小元 n.
断言 $H=\langle g^n\rangle$. 对任意 $g^m\in H$, 带余除法写 $m=qn+r$, $0\le r<n$. 则

$$g^r=g^m(g^n)^{-q}\in H.$$

由 n 的最小性, $r=0$. 故 m 是 n 的倍数, $g^m\in\langle g^n\rangle$. 反向包含 $\langle g^n\rangle\subseteq H$ 显然. 故 $H=\langle g^n\rangle$ 是循环群.
与 $\mathbb{Z}^+$ 的联系: 满同态 $\phi:\mathbb{Z}^+\to G$, $k\mapsto g^k$, 其核是 $\mathbb{Z}^+$ 的某个子群. 而 $\mathbb{Z}^+$ 的子群均已描述为 $n\mathbb{Z}^+=\langle n\rangle$ (即由单个整数 n 生成的循环群). 设 H 的原像 $\phi^{-1}(H)$ 就是这个 $\langle n\rangle$, 则由满同态下像与原像的对应, $H=\phi(\langle n\rangle)=\langle g^n\rangle$ 循环, 与上面用指数直接证明的结果一致.

习题 6.7

Let H be a subgroup of G, and let g be a fixed element of G. The conjugate subgroup gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, with h in H. Prove that gHg^{-1} is a subgroup of G.

解答

题目翻译: 设 H 是 G 的子群, g 是 G 的固定元素. 共轭子群 gHg^{-1} 定义为所有共轭 ghg^{-1} $(h \in H)$ 的集合. 证明 gHg^{-1} 是 G 的子群.

解答: 方法一: 共轭映射 $c_g : G \to G$, $x \mapsto gxg^{-1}$, 是自同构: 它是同态, 因为

$$(gxg^{-1})(gyg^{-1}) = g(xy)g^{-1},$$

且逆映射为 $c_{g^{-1}}$, 故为双射. 子群在同态下的像是子群, 故 $c_g(H) = gHg^{-1}$ 是 G 的子群.

方法二 (直接验证): $1 = g1g^{-1} \in gHg^{-1}$. 若 gh_1g^{-1}, $gh_2g^{-1} \in gHg^{-1}$, 则

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1};$$

又 $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$. 故 gHg^{-1} 是子群.

习题 6.8

Prove that the map $A \mapsto (A^t)^{-1}$ is an automorphism of $\mathrm{GL}_n(R)$.

解答

题目翻译: 证明映射 $A \mapsto (A^t)^{-1}$ 是 $\mathrm{GL}_n(R)$ 的自同构.

解答: 记 $T(A) = (A^t)^{-1}$. 对 $A, B \in \mathrm{GL}_n(R)$,

$$T(AB) = ((AB)^t)^{-1} = (B^tA^t)^{-1} = (A^t)^{-1}(B^t)^{-1} = T(A)T(B),$$

其中第二步用到转置的反序性, 第三步用到 $(XY)^{-1} = Y^{-1}X^{-1}$. 故 T 是同态.

再利用 $(A^t)^{-1} = (A^{-1})^t$,

$$T(T(A)) = T\big((A^t)^{-1}\big) = \big(((A^t)^{-1})^t\big)^{-1} = \big(((A^{-1})^t)^t\big)^{-1} = (A^{-1})^{-1} = A.$$

故 $T^2 = \mathrm{id}$, T 是双射. 因此 T 是 $\mathrm{GL}_n(R)$ 的自同构.

习题 7.2

An equivalence relation on S is determined by the subset R of the set $S \times S$ consisting of those pairs (a, b) such that $a \sim b$. Write the axioms for an equivalence relation in

terms of the subset R.

解答

题目翻译: S 上的等价关系由 $S \times S$ 的子集 R 决定, 其中 R 由所有满足 $a \sim b$ 的数对 (a, b) 组成. 用子集 R 写出等价关系的各条公理.

解答: 反身性: 对一切 $a \in S$, $(a, a) \in R$. 等价地, 对角线 $\Delta = \{(a, a) : a \in S\} \subseteq R$.
对称性: 若 $(a, b) \in R$, 则 $(b, a) \in R$. 记 $R^{-1} = \{(b, a) : (a, b) \in R\}$, 此条即 $R^{-1} \subseteq R$; 由对称性两边各用一次得 $R \subseteq R^{-1}$, 故等价于 $R = R^{-1}$.
传递性: 若 $(a, b) \in R$ 且 $(b, c) \in R$, 则 $(a, c) \in R$. 记 $R \circ R = \{(a, c) : 存在 b \in S, (a, b) \in R 且 (b, c) \in R\}$, 此条即 $R \circ R \subseteq R$.
这三条合起来就是 R 成为等价关系 (即 $\sim$ 为等价关系) 的充要条件.

习题 8.7

A group G of order 22 contains elements x and y, where $x \neq 1$ and y is not a power of x. Prove that the subgroup generated by these elements is the whole group G.

解答

题目翻译: 22 阶群 G 含有元素 x 与 y, 其中 $x \neq 1$, 且 y 不是 x 的幂. 证明由这两个元素生成的子群是整个群 G.

解答: 记 $H = \langle x, y \rangle$. 由 Lagrange 定理, $|x|$ 整除 $22 = 2 \times 11$ 且 $|x| \neq 1$, 故 $|x| \in \{2, 11, 22\}$.
若 $|x| = 22$, 则 $\langle x \rangle = G$, G 的每个元素都是 x 的幂, 与 y 不是 x 的幂矛盾. 故 $|x| \neq 22$.
若 $|x| = 11$, 则 $H \supseteq \langle x \rangle$, 故 $|H| \geq 11$ 且 $|H|$ 整除 22. 若 $|H| = 11$, 则 $H = \langle x \rangle$, 从而 $y \in \langle x \rangle$, 矛盾. 故 $|H| = 22 = |G|$, $H = G$.
若 $|x| = 2$, 则 $H \supseteq \{1, x\}$, $|H| \geq 2$ 且 $|H|$ 整除 22, 故 $|H| \in \{2, 11, 22\}$. 若 $|H| = 2$, 则 $H = \{1, x\}$, $y \in \{1, x\}$, 即 $y = 1 = x^0$ 或 $y = x = x^1$, 都是 x 的幂, 矛盾. 若 $|H| = 11$, 由 Lagrange 定理, $2 = |\langle x \rangle|$ 应整除 11, 矛盾. 故 $|H| = 22$, $H = G$.
综上, 各种情形下都有 $H = G$.

习题 8.9

Let G be a finite group. Under what circumstances is the map $\phi : G \to G$ defined by $\phi(x) = x^2$ an automorphism of G?

解答

题目翻译: 设 G 是有限群. 在什么条件下, 由 $\phi(x) = x^2$ 定义的映射 $\phi : G \to G$ 是 G 的自同构?

解答: ϕ 是自同构的首要条件是它是同态. 若 ϕ 是同态, 则对任意 $x, y \in G$,

$$(xy)^2 = x^2y^2, \quad \text{即} xyxy = xxyy.$$

两边左乘 x^{-1}, 右乘 y^{-1}, 得 $yx = xy$. 故 G 交换. 反之, 若 G 交换, 则

$$\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y),$$

ϕ 是同态. 所以 G 交换是 ϕ 为同态的充要条件.
在 G 交换的前提下, ϕ 的核为

$$\ker\phi = \{x \in G : x^2 = 1\} = \{x \in G : |x| \le 2\}.$$

有限群的自同态是自同构当且仅当它是单射 (有限集上的单射必为双射), 当且仅当 $\ker\phi = \{1\}$. 故条件为: G 中没有 2 阶元.
对有限群, 没有 2 阶元等价于 $|G|$ 为奇数: 若 $|G|$ 为偶数, 将元素按 $\{x, x^{-1}\}$ 配对, 满足 $x^2 = 1$ 的元素恰是不配对的元素, 它们连同 1 成偶数个 (因 $|G|$ 偶数), 故除 1 外还必有非平凡的 2 阶元; 若 $|G|$ 为奇数, 由 Lagrange 定理不可能有 2 阶元.
所以 ϕ 是自同构当且仅当 G 是奇数阶交换群.

习题 8.10

Prove that every subgroup of index 2 is a normal subgroup, and show by example that a subgroup of index 3 need not be normal.

解答

题目翻译: 证明每个指数为 2 的子群都是正规子群, 并举例说明指数为 3 的子群不必是正规的.
解答: 设 $H \le G$, $[G : H] = 2$. 对任意 $g \in G$: 若 $g \in H$, 则 $gH = H = Hg$. 若 $g \notin H$, 则 gH 与 H 是仅有的两个左陪集, 故 $gH = G \setminus H$; 同理 Hg 也是 H 之外的那个右陪集, 即 $Hg = G \setminus H$. 于是 $gH = Hg$, 故 $gHg^{-1} = H$. 所以 H 是正规子群.
反例: 取 $G = S_3$, $H = \{1, (12)\}$. 则 $[S_3 : H] = 6/2 = 3$. 但 H 不正规, 例如

$$(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin H.$$

故指数为 3 的子群未必正规.

习题 9.6

Prove the Chinese Remainder Theorem: Let a, b, u, v be integers, and assume that the greatest common divisor of a and b is 1. Then there is an integer x such that $x \equiv u \pmod{a}$ and $x \equiv v \pmod{b}$. Hint: Do the case $u = 0$ and $v = 1$ first.

解答

题目翻译: 证明中国剩余定理: 设 a, b, u, v 是整数, 且 a 与 b 的最大公因数为 1. 则存在整数 x 使得 $x \equiv u \pmod{a}$ 且 $x \equiv v \pmod{b}$. 提示: 先做 $u = 0$, $v = 1$ 的情形.
解答: 先做 $u = 0$, $v = 1$ 的情形. 因 $\gcd(a, b) = 1$, 由 Bezout 定理, 存在整数 m, n 使

$$ma + nb = 1.$$

令 $x_0 = ma$. 则 $x_0 = ma \equiv 0 \pmod{a}$; 又 $x_0 = ma = 1 - nb \equiv 1 \pmod{b}$. 故 x_0 满足 $x_0 \equiv 0 \pmod{a}$, $x_0 \equiv 1 \pmod{b}$. 同理, $x_1 = nb$ 满足

$$x_1 \equiv 1 \pmod{a}, \qquad x_1 \equiv 0 \pmod{b}.$$

对一般情形, 取

$$x = u\,x_1 + v\,x_0.$$

模 a: $x \equiv u \cdot 1 + v \cdot 0 = u$; 模 b: $x \equiv u \cdot 0 + v \cdot 1 = v$. 故 x 满足要求.
(唯一性) 若 x' 也满足这两个同余式, 则 a 与 b 均整除 $x - x'$. 因 $\gcd(a, b) = 1$, ab 整除 $x - x'$, 故 $x \equiv x' \pmod{ab}$. 即解在模 ab 意义下唯一.

习题 10.2

Let H and K be subgroups of a group G. (a) Prove that the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$. (b) Prove that if H and K have finite index in G then $H \cap K$ also has finite index in G.

解答

题目翻译: 设 H 与 K 是群 G 的子群. (a) 证明 H 的陪集 xH 与 K 的陪集 yK 的交集要么为空, 要么是子群 $H \cap K$ 的一个陪集. (b) 证明若 H 与 K 在 G 中的指数有限, 则 $H \cap K$ 在 G 中的指数也有限.
解答: (a) 若 $xH \cap yK = \varnothing$, 无事可证. 否则取 $z \in xH \cap yK$, 则 $z = xh_1 = yk_1$ ($h_1 \in H$, $k_1 \in K$). 断言

$$xH \cap yK = z(H \cap K).$$

先证 $\subseteq$: 对 $w \in xH \cap yK$, 设 $w = xh_2 = yk_2$. 则

$$z^{-1}w = (xh_1)^{-1}(xh_2) = h_1^{-1}h_2 \in H,$$

且 $z^{-1}w = (yk_1)^{-1}(yk_2) = k_1^{-1}k_2 \in K$. 故 $z^{-1}w \in H \cap K$, 即 $w \in z(H \cap K)$.
再证 $\supseteq$: $z(H \cap K) = xh_1(H \cap K) \subseteq xH$ (因 $H \cap K \subseteq H$), 且 $z(H \cap K) = yk_1(H \cap K) \subseteq yK$ (因 $H \cap K \subseteq K$). 故 $z(H \cap K) \subseteq xH \cap yK$.
于是 $xH \cap yK$ 是 $H \cap K$ 的陪集 $z(H \cap K)$.

(b) 考虑映射

$$f : G/(H \cap K) \to G/H \times G/K, \qquad g(H \cap K) \mapsto (gH,\ gK).$$

它是良定的: 若 $g(H \cap K) = g'(H \cap K)$, 则 $g'^{-1}g \in H \cap K \subseteq H,\ K$, 故 $gH = g'H$, $gK = g'K$. 它单射: 若 $gH = g'H$ 且 $gK = g'K$, 则 $g'^{-1}g \in H \cap K$, 故 $g(H \cap K) = g'(H \cap K)$. 于是

$$|G/(H \cap K)| \le |G/H| \cdot |G/K| = [G : H][G : K] < \infty.$$

故 $[G : H \cap K]$ 有限, 且有不等式 $[G : H \cap K] \le [G : H][G : K]$.

习题 11.6

Let G be a group that contains normal subgroups of orders 3 and 5, respectively. Prove that G contains an element of order 15.

解答

题目翻译: 设 G 是含有阶分别为 3 和 5 的两个正规子群的群. 证明 G 含有 15 阶元素.

解答: 设 $H \trianglelefteq G$, $|H| = 3$; $K \trianglelefteq G$, $|K| = 5$. 因 3 与 5 互素, 由 Lagrange 定理, $|H \cap K|$ 整除 $\gcd(3, 5) = 1$, 故 $H \cap K = \{1\}$. 又 H, K 均正规, 积集 HK 是 G 的子群, 且

$$|HK| = \frac{|H||K|}{|H \cap K|} = 15.$$

下面证 H 与 K 的元素两两交换. 对 $h \in H$, $k \in K$, 考虑换位子 $[h, k] = hkh^{-1}k^{-1}$. 因 K 正规, $hkh^{-1} \in K$, 故 $[h, k] = (hkh^{-1})k^{-1} \in K$; 因 H 正规, $kh^{-1}k^{-1} \in H$, 故 $[h, k] = h(kh^{-1}k^{-1}) \in H$. 于是 $[h, k] \in H \cap K = \{1\}$, 即 $hk = kh$.

因此 $HK \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. 因 $\gcd(3, 5) = 1$, 乘积 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ 是循环群 (元素 $(\bar{1}, \bar{1})$ 的阶为 $\operatorname{lcm}(3, 5) = 15$), 故 HK 是 15 阶循环群, 其生成元是 15 阶元素. 于是 G 含有 15 阶元素.

习题 11.7

Let H be a subgroup of a group G, let $\phi : G \to H$ be a homomorphism whose restriction to H is the identity map, and let N be its kernel. What can one say about the product map $H \times N \to G$?

解答

题目翻译: 设 H 是群 G 的子群, $\phi: G \to H$ 是同态, 且 ϕ 限制在 H 上是恒等映射, 设 N 是 ϕ 的核. 关于积映射 $H \times N \to G$, 能得出什么结论?

解答: 记积映射 $\mu: H \times N \to G$, $(h, n) \mapsto hn$. 首先, μ 是双射. 分三步证明.

(i) $H \cap N = \{1\}$: 若 $x \in H \cap N$, 则 $\phi(x) = x$ (因 $x \in H$) 且 $\phi(x) = 1$ (因 $x \in N$), 故 $x = 1$.

(ii) $G = HN$: 对任意 $g \in G$, 令 $h = \phi(g) \in H$. 则

$$\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = h \cdot h^{-1} = 1,$$

故 $gh^{-1} \in N$, 即 $g = (gh^{-1})h \in NH$. 于是 $G = NH$. 因 N 是核, 必正规, 故 $NH = HN$, 即 $G = HN$.

(iii) μ 单射: 若 $h_1 n_1 = h_2 n_2$, 则 $h_2^{-1} h_1 = n_2 n_1^{-1} \in H \cap N = \{1\}$, 故 $h_1 = h_2$, $n_1 = n_2$. μ 满射由 $G = HN$ 保证.

所以每个 $g \in G$ 有唯一分解 $g = hn$ ($h \in H$, $n \in N$), μ 是集合之间的双射, 即 G 是 N 与 H 的半直积.

但 μ 未必是同态: 一方面

$$\mu\Big((h_1, n_1)(h_2, n_2)\Big) = \mu(h_1 h_2,\ n_1 n_2) = h_1 h_2\, n_1 n_2,$$

另一方面

$$\mu(h_1, n_1)\, \mu(h_2, n_2) = h_1 n_1\, h_2 n_2.$$

这两个表达式对一切 $h_1, h_2 \in H$, $n_1, n_2 \in N$ 相等, 当且仅当 $nh = hn$ 对一切 $h \in H$, $n \in N$ 成立, 即 H 与 N 逐元素交换. 此时 μ 是同构, $G \cong H \times N$; 一般情况下 G 只是半直积, μ 仅为双射.

反例说明一般情形: $G = S_3$, $H = \{1, (12)\}$, $N = A_3 = \{1, (123), (132)\}$. 商 $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, 复合投影得到 $\phi: S_3 \to H$, 其限制在 H 上恒等, 核为 N. 但 $S_3 \ncong H \times N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (后者交换, 前者非交换), 此时 μ 是双射而非同态.

2

第二次作业

习题 12.1

Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.

解答

题目翻译: 证明: 若群 G 的子群 H 不是正规子群, 则存在左陪集 aH 与 bH, 它们的乘积 (集合 $\{xy : x \in aH,\ y \in bH\}$) 不再是 G 的某个左陪集.

解答: 反证. 设 H 不正规, 则存在 $a \in G$ 与 $h \in H$ 使 $aha^{-1} \notin H$. 考虑两个左陪集 aH 与 $a^{-1}H$ 的乘积 $(aH)(a^{-1}H)$. 这个集合含有 $a \cdot a^{-1} = 1$ (取 $x = a$, $y = a^{-1}$), 也含有 $(ah)a^{-1} = aha^{-1}$ (取 $x = ah$, $y = a^{-1}$). 若 $(aH)(a^{-1}H)$ 是某个左陪集 cH, 则由 $1 \in cH$ 知 $1 = ch$ 对某 $h \in H$, 从而 $c = h^{-1} \in H$, 故 $cH = H$. 于是 $aha^{-1} \in H$, 与 $aha^{-1} \notin H$ 矛盾. 因此 $(aH)(a^{-1}H)$ 不是陪集, 取 $b = a^{-1}$ 即得结论. 这里用到陪集的基本事实: $x \in cH$ 当且仅当 $xH = cH$.

习题 12.2

In the general linear group $\mathrm{GL}_3(R)$, consider the subsets $H = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$, $K = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$, where $*$ represents an arbitrary real number. Show that H is a subgroup of GL_3, that K is a normal subgroup of H, and identify the quotient group H/K. Determine the center of H.

解答

题目翻译: 在一般线性群 $\mathrm{GL}_3(R)$ 中, 考虑子集 H (对角线全为 1 的上三角矩阵) 与 K (仅 $(1,3)$ 位置任意取实的矩阵). 证明 H 是 GL_3 的子群, K 是 H 的正规子群, 并识别商群 H/K; 再求 H 的中心.

解答: 记 $M(a,b,c)=\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix}$, 则 $H=\{M(a,b,c):a,b,c\in R\}$, $K=\{M(0,0,c)\}$.
直接计算矩阵乘法得

$$M(a,b,c)\,M(a',b',c')=M(a+a',\ b+b',\ c+c'+ab').$$

单位元为 $M(0,0,0)$, 且 $M(a,b,c)^{-1}=M(-a,-b,\,-c+ab)$, 故 H 对乘法与取逆封闭, 是 $\mathrm{GL}_3(R)$ 的子群.
K 是 H 的子群: $M(0,0,c)M(0,0,c')=M(0,0,c+c')$. 又

$$M(a,b,c)\,M(0,0,k)\,M(a,b,c)^{-1}=M(0,0,k),$$

故 K 中每个元素与 H 的一切元素交换, 所以 $K\lhd H$ (事实上含于中心).
商群 H/K: 陪集 $M(a,b,c)K$ 由 (a,b) 唯一确定, 乘法律为 $M(a,b)\,M(a',b')=M(a+a',b+b')$, 恰与加法群 $R\times R$ 的运算一致, 故 $H/K\cong R\times R$ (加法群).
中心: 若 $M(a,b,c)$ 与一切 $M(a',b',c')$ 交换, 比较两个乘积的 $(1,3)$ 分量得 $ab'=a'b$ 对一切 $a',b'\in R$ 成立. 取 $a'=1,b'=0$ 得 $b=0$; 取 $a'=0,b'=1$ 得 $a=0$. 故中心恰为 $\{M(0,0,c)\}=K\cong R$.

习题 1.6

Decide whether or not S is a subring of R, when
(a) S is the set of all rational numbers a/b, where b is not divisible by 3, and $R=\mathbb{Q}$,
(b) S is the set of functions which are linear combinations with integer coefficients of the functions $\{1,\cos nt,\sin nt\}$, $n\in\mathbb{Z}$, and R is the set of all real valued functions of t.

解答

题目翻译: 判断下列 S 是否构成 R 的子环: (a) S 是分母不被 3 整除的一切有理数 a/b 的集合, $R=\mathbb{Q}$; (b) S 是函数族 $\{1,\cos nt,\sin nt\}$, $n\in\mathbb{Z}$ 的整数系数线性组合所成集合, R 是一切实值函数的集合.
解答:(a) 是子环. $1=1/1\in S$. 对 $a/b,c/d\in S$ (即 $3\nmid b$, $3\nmid d$), 差 $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$ 与积 $\frac{ac}{bd}$ 的分母都不被 3 整除 (因 $3\nmid bd$), 故 S 对减法与乘法封闭, 是 $\mathbb{Q}$ 的子环. 此即整数环在素数 3 处的局部化 $\mathbb{Z}_{(3)}$.
(b) 不是子环, 因为乘法不封闭. 例如 $\cos t\in S$, 而 $\cos^2 t=\frac{1+\cos 2t}{2}$ 需要系数 $\frac{1}{2}$. 若 $\cos^2 t\in S$, 则 $1+\cos 2t=2c_0+\sum_n(2c_n\cos nt+2d_n\sin nt)$ (c_n,d_n 为整数); 由函数族 $\{1,\cos nt,\sin nt\}$ 的线性无关性, 比较常数项得 $2c_0=1$, 不可能. 所以 $\cos^2 t\notin S$, S 对乘法不封闭.

习题 1.7

Decide whether the given structure forms a ring. If it is not a ring, determine which of the ring axioms hold and which fail:
(a) U is an arbitrary set, and R is the set of subsets of U. Addition and multiplication are defined by $A + B = (A \cup B) - (A \cap B)$ and $A \cdot B = A \cap B$.
(b) R is the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Addition and multiplication are defined by $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.

解答

题目翻译: 判断下列结构是否为环. 若不是环, 指出哪些环公理成立, 哪些不成立: (a) U 为任意集合, R 为 U 的全体子集, 加法与乘法分别为对称差 $A+B = (A\cup B)-(A\cap B)$ 与交集 $A\cdot B = A\cap B$; (b) R 为连续函数 $\mathbb{R} \to \mathbb{R}$ 的集合, 加法为逐点相加 $[f+g](x) = f(x)+g(x)$, 乘法为函数复合 $[f \circ g](x) = f(g(x))$.
解答:(a) 是环 (布尔环). 加法即对称差 $A\triangle B$: 空集 $\varnothing$ 是零元, 且 $A + A = \varnothing$, 故 $-A = A$; 对称差满足交换律与结合律. 乘法为交集, 交换且结合, 单位元为 U (因 $A \cap U = A$). 分配律成立, 因为交对对称差可分配:

$$A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C).$$

每个元素幂等 ($A \cdot A = A$), 该环特征为 2.
(b) 不是环. 加法: 连续函数在逐点加法下构成 Abel 群 (零函数为零元, 负元为取负). 乘法 (复合) 结合, 且有单位元 (恒等函数). 但左分配律不成立: 取 $f(x) = x^2$, $g(x) = h(x) = x$, 则

$$f \circ (g + h)(x) = (2x)^2 = 4x^2, \qquad (f \circ g + f \circ h)(x) = x^2 + x^2 = 2x^2,$$

两者不相等. 所以乘法对加法不满足 (左) 分配律, 不是环. (右分配律 $(g + h) \circ f = g \circ f + h \circ f$ 成立.)

习题 2.1

For which positive integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 7x + 5$ in $\mathbb{Z}/(n)[x]$?

解答

题目翻译: 对哪些正整数 n, 在 $\mathbb{Z}/(n)[x]$ 中 $x^2 + x + 1$ 整除 $x^4 + 3x^3 + x^2 + 7x + 5$?
解答: 先在 $\mathbb{Z}[x]$ 中对 $x^4 + 3x^3 + x^2 + 7x + 5$ 除以首一多项式 $x^2 + x + 1$ 做带余除法:

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + x + 1)(x^2 + 2x - 2) + (7x + 7).$$

该等式在 $\mathbb{Z}/(n)[x]$ 中仍成立. 在 $\mathbb{Z}/(n)[x]$ 中整除当且仅当余式 $7x+7$ 为零多项式, 即

系数 $7 \equiv 0 \pmod{n}$, 亦即 $n \mid 7$. 故 $n = 7$ (对 $n \geq 2$; 若允许 $n = 1$, 则 $\mathbb{Z}/(1)$ 是零环, 情形平凡). 答案: $n = 7$.

习题 3.3

Find generators for the kernels of the following maps:
(a) $R[x, y] \to \mathbb{R}$ defined by $f(x, y) \mapsto f(0, 0)$,
(b) $R[x] \to \mathbb{C}$ defined by $f(x) \mapsto f(2 + i)$,
(c) $\mathbb{Z}[x] \to \mathbb{R}$ defined by $f(x) \mapsto f(1 + \sqrt{2})$,
(d) $\mathbb{Z}[x] \to \mathbb{C}$ defined by $x \mapsto \sqrt{2} + \sqrt{3}$,
(e) $\mathbb{C}[x, y, z] \to \mathbb{C}[t]$ defined by $x \mapsto t$, $y \mapsto t^2$, $z \mapsto t^3$.

解答

题目翻译: 求下列映射的核的一组生成元.
解答:(a) 核是原点处取值为 0 的多项式, 即常数项为 0 的多项式, 恰由 x, y 生成: $\ker = (x, y)$.
(b) 映射是 $f \mapsto f(2 + i)$. $2 + i$ 是 $x^2 - 4x + 5 = (x - (2 + i))(x - (2 - i))$ 的根, 而 $x^2 - 4x + 5$ 在 $\mathbb{R}$ 上不可约 (判别式 $-4 < 0$). $\mathbb{R}[x]$ 是主理想整环, 不可约多项式生成极大理想; 核是含 $(x^2 - 4x + 5)$ 的真理想, 故 $\ker = (x^2 - 4x + 5)$.
(c) 代入 $x = 1 + \sqrt{2}$. 该数是 $x^2 - 2x - 1$ 的根 (因 $(1 + \sqrt{2})^2 - 2(1 + \sqrt{2}) - 1 = 0$), 而 $x^2 - 2x - 1$ 无整数根, 在 $\mathbb{Z}[x]$ 中不可约. 对 $f \in \ker$, 用首一多项式 $x^2 - 2x - 1$ 做带余除法得 $f = (x^2 - 2x - 1)q + (ax + b)$; 代入 $1 + \sqrt{2}$ 得 $a(1 + \sqrt{2}) + b = 0$, 即 $a = b = 0$. 故 $\ker = (x^2 - 2x - 1)$.
(d) 记 $\alpha = \sqrt{2} + \sqrt{3}$. 则 $\alpha^2 = 5 + 2\sqrt{6}$, $(\alpha^2 - 5)^2 = 24$, 即 $\alpha^4 - 10\alpha^2 + 1 = 0$. 又 $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$, 故 $\sqrt{2} = (\alpha^3 - 9\alpha)/2$, $\sqrt{3} = \alpha - \sqrt{2}$, 所以 $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 $\mathbb{Q}$ 的 4 次扩张, α 的最小多项式次数为 4. 首一 4 次多项式 $x^4 - 10x^2 + 1$ 以 α 为根, 故它就是最小多项式. 对 $f \in \ker$ 除以它 (首一) 的余式次数 ≤ 3, 以 α 为根必为零, 故 $\ker = (x^4 - 10x^2 + 1)$.
(e) 即三次挠曲线 $t \mapsto (t, t^2, t^3)$ 的核. 显然 $y - x^2$, $z - x^3$ 都映到 0, 故 $(y - x^2, z - x^3) \subseteq \ker$. 反之, 对 $f \in \ker$, 反复用关系 $y = x^2$, $z = x^3$ 把 f 化为只含 x 的多项式 $g(x)$, 即

$$f = g(x) + (y - x^2)A + (z - x^3)B.$$

代入映射得 $g(t) = 0$ 在 $\mathbb{C}[t]$ 中, 故 $g = 0$. 于是 $f \in (y - x^2, z - x^3)$. 所以 $\ker = (y - x^2, z - x^3)$.

习题 3.9

(a) An element x of a ring R is called nilpotent if some power is zero. Prove that if x is nilpotent, then $1 + x$ is a unit.

(b) Suppose that R has prime characteristic $p \neq 0$. Prove that if a is nilpotent then $1+a$ is unipotent, that is, some power of $1+a$ is equal to 1.

解答

题目翻译:(a) 环 R 的元素 x 称为幂零的, 若某次幂为零. 证明: 若 x 幂零, 则 $1+x$ 是单位. (b) 设 R 有素数特征 $p \neq 0$. 证明: 若 a 幂零, 则 $1+a$ 是幂幺的, 即 $1+a$ 的某次幂等于 1.

解答:(a) 设 $x^n = 0$. 由等比数列求和公式,

$$(1+x)\left(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1}\right) = 1+(-1)^{n-1}x^n = 1.$$

故 $1+x$ 可逆, 逆为 $1-x+x^2-\cdots+(-1)^{n-1}x^{n-1}$.

(b) 设 R 为交换环 (环论部分均按交换环讨论), 特征为素数 p. 二项式定理给出

$$(1+a)^{p^k} = \sum_{j=0}^{p^k} \binom{p^k}{j} a^j.$$

当 $1 \leq j \leq p^k-1$ 时, $\binom{p^k}{j} = \frac{p^k(p^k-1)\cdots(p^k-j+1)}{j!}$ 被 p 整除 (因为 p 是素数, $j!$ 不含因子 p, 而分子含 p^k), 特征 p 使 $p \cdot c = 0$, 故这些中间项全部为零. 于是

$$(1+a)^{p^k} = 1+a^{p^k}.$$

设 $a^n = 0$, 取 k 使 $p^k \geq n$, 则 $a^{p^k} = a^n \cdot a^{p^k-n} = 0$, 得 $(1+a)^{p^k} = 1$. 故 $1+a$ 幂幺.

习题 3.12

Let I and J be ideals of a ring R. Prove that the set $I+J$ of elements of the form $x+y$, with x in I and y in J, is an ideal. This ideal is called the sum of the ideals I and J.

解答

题目翻译: 设 I, J 是环 R 的理想. 证明: 形如 $x+y$ ($x \in I$, $y \in J$) 的元素全体 $I+J$ 构成 R 的理想. 该理想称为 I 与 J 的和.

解答: 用理想判定条件逐条验证. (i) $0 = 0+0 \in I+J$, 非空. (ii) 对 x_1+y_1, $x_2+y_2 \in I+J$, 差

$$(x_1+y_1)-(x_2+y_2) = (x_1-x_2)+(y_1-y_2) \in I+J,$$

因为 I, J 对减法封闭. (iii) 对 $r \in R$, $x \in I$, $y \in J$, 有 $rx \in I$, $ry \in J$, 故

$$r(x+y) = rx+ry \in I+J,$$

同理 $(x+y)r \in I+J$. 所以 $I+J$ 对加法与两侧吸收封闭, 是 R 的理想. 事实上 $I+J$ 是同时包含 I 与 J 的最小理想.

习题 4.2

What does the Correspondence Theorem tell us about ideals of $\mathbb{Z}[x]$ that contain x^2+1?

解答

题目翻译: 对应定理 (Correspondence Theorem) 对含 x^2+1 的 $\mathbb{Z}[x]$ 的理想给出什么结论?

解答: 对应定理 (或第一同构定理的推论) 说: 对满同态 $\mathbb{Z}[x] \to \mathbb{Z}[x]/(x^2+1)$, 商环 $\mathbb{Z}[x]/(x^2+1)$ 的理想与 $\mathbb{Z}[x]$ 中含 (x^2+1) 的理想之间有一一对应 (对应为 $J \mapsto J/(x^2+1)$, 其逆为取原像). 而 $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$ (Gauss 整数环, 同构 $x \mapsto i$). Gauss 整数环以范 $N(a+bi) = a^2+b^2$ 为 Euclid 函数, 是 Euclid 整环, 从而是主理想整环: 每个理想都由一个元素 $a+bi$ 生成. 模 x^2+1 后每个多项式可降到次数不超过 1 的形式, 所以这些理想在 $\mathbb{Z}[x]$ 中的原像都是

$$(x^2+1,\ a+bx), \qquad a,b \in \mathbb{Z},$$

由 x^2+1 与一个一次多项式 $a+bx$ 共同生成. 其中 $a=b=0$ 对应理想 (x^2+1) 本身 (即 $\mathbb{Z}[i]$ 的零理想); $a+bx$ 为 ± 1 时整个理想为 $\mathbb{Z}[x]$, 对应 $\mathbb{Z}[i]$ 本身. 结论: 含 x^2+1 的 $\mathbb{Z}[x]$ 的理想一一对应于 $\mathbb{Z}[i]$ 的主理想, 且每个都形如 $(x^2+1,\ a+bx)$.

习题 4.4

Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?

解答

题目翻译: 环 $\mathbb{Z}[x]/(x^2+7)$ 与 $\mathbb{Z}[x]/(2x^2+7)$ 是否同构?

解答: 不同构. 记 $R_1 = \mathbb{Z}[x]/(x^2+7)$, $R_2 = \mathbb{Z}[x]/(2x^2+7)$. 在 R_2 中, 关系 $2x^2 = -7$ 给出

$$2\,(-x^2-3) = -2x^2-6 = 7-6 = 1,$$

所以 2 在 R_2 中可逆, 逆为 $-x^2-3$. 在 R_1 中, 每个元素都可写成 $a+b\bar{x}$ $(a,b \in \mathbb{Z})$; 若 $2(a+b\bar{x}) = 1$, 则 $2a=1$, 这在 $\mathbb{Z}$ 中无解, 故 2 在 R_1 中不可逆. 元素是否可逆在同构下保持不变, 所以 $R_1 \not\cong R_2$.

习题 5.1

Let $f = x^4+x^3+x^2+x+1$ and let α denote the residue of x in the ring $R = \mathbb{Z}[x]/(f)$. Express $(\alpha^3+\alpha^2+\alpha)(\alpha^5+1)$ in terms of the basis $(1, \alpha, \alpha^2, \alpha^3)$ of R.

解答

题目翻译: 设 $f = x^4 + x^3 + x^2 + x + 1$, α 是 x 在环 $R = \mathbb{Z}[x]/(f)$ 中的剩余类. 把 $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$ 写成 R 的基 $(1, \alpha, \alpha^2, \alpha^3)$ 下的线性组合.
解答: 由恒等式 $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ 及 $f(\alpha) = 0$ 得

$$\alpha^5 - 1 = (\alpha - 1)f(\alpha) = 0,$$

即 $\alpha^5 = 1$. 于是

$$(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1) = (\alpha^3 + \alpha^2 + \alpha)(1 + 1) = 2\alpha^3 + 2\alpha^2 + 2\alpha.$$

答案: $2\alpha^3 + 2\alpha^2 + 2\alpha$, 即基 $(1, \alpha, \alpha^2, \alpha^3)$ 下的坐标 $(0, 2, 2, 2)$.

习题 5.3

Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2.

解答

题目翻译: 描述在 $\mathbb{Z}/12\mathbb{Z}$ 中添加 2 的逆所得的环.
解答: 该环是 $R' = (\mathbb{Z}/12\mathbb{Z})[x]/(2x - 1)$, 记 $\alpha = x$, 则 $2\alpha = 1$. 在 R' 中 $12 = 0$, 于是

$$6 = 6 \cdot (2\alpha) = 12\alpha = 0,$$

故 $6 = 0$. 设 $\pi : \mathbb{Z}/12\mathbb{Z} \to R'$ 为自然映射. 由习题 5.6(b), $\ker \pi = \{b \in \mathbb{Z}/12\mathbb{Z} : 2^n b = 0 \text{ 对某} n > 0\}$, 计算得 $\ker \pi = \{0, 3, 6, 9\}$. 故 π 的像是 $\mathbb{Z}/12\mathbb{Z}/\{0, 3, 6, 9\} \cong \mathbb{Z}/3\mathbb{Z}$. 在 $\mathbb{Z}/3\mathbb{Z}$ 中, 2 的逆是 2 (因 $2 \cdot 2 = 4 = 1$), 已包含在像中, 故 R' 由该像生成. 所以 $R' \cong \mathbb{Z}/3\mathbb{Z}$.
另一途径: $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; 在 $\mathbb{Z}/4\mathbb{Z}$ 中 2 幂零 ($2^2 = 0$), 求逆把该分量压成零环; 在 $\mathbb{Z}/3\mathbb{Z}$ 中 2 已是单位, 分量不变. 结果同样是 $\mathbb{Z}/3\mathbb{Z}$.

习题 5.7

Let F be a field and let $R = F[t]$ be the polynomial ring. Let R' be the ring extension $R[x]/(tx - 1)$ obtained by adjoining an inverse of t to R. Prove that this ring can be identified as the ring of Laurent polynomials, which are finite linear combinations of powers of t, negative exponents included.

解答

题目翻译: 设 F 是域, $R = F[t]$ 是多项式环, $R' = R[x]/(tx - 1)$ 是在 R 中添加 t 的逆所得扩环. 证明该环可等同于 Laurent 多项式环 (即 t 的幂的有限线性组合, 允许负指数).

解答: 记 $F[t,t^{-1}]$ 为 Laurent 多项式环. 由代入原理定义环同态

$$\varphi : R' = F[t][x]/(tx-1) \longrightarrow F[t,t^{-1}], \qquad t \mapsto t,\ x \mapsto t^{-1}.$$

良定义: 生成关系 $tx-1$ 映到 $t\cdot t^{-1}-1=0$. 满: $F[t,t^{-1}]$ 由 t 与 t^{-1} 生成, 而它们是 φ 的像. 单: 把 $h\in R'$ 写成 Laurent 形式 $h=\sum_{i=-m}^{n} c_i t^i$ ($c_i\in F$, 有限和), 则 $\varphi(h)=0$ 给出 $t^{-m}(\sum_{i=-m}^{n} c_i t^{i+m})=0$; 因 $F[t,t^{-1}]$ 是整环且 t^{-m} 可逆, 故 $\sum_i c_i t^{i+m}=0$, 从而各 $c_i=0$. 所以 φ 是单射, 从而是同构 $R'\cong F[t,t^{-1}]$.
直观地说, 关系 $tx=1$ 给出 $x=t^{-1}$; 每个元素 $\sum_i a_i(t)x^i$ 经 $x^i=t^{-i}$ 展开为 $\sum_k c_k t^k$ ($k\in\mathbb{Z}$ 有限), 即 Laurent 多项式, 唯一性由上面的单射性保证.

习题 6.1

Let $\varphi : \mathbb{R}[x] \to \mathbb{C}\times\mathbb{C}$ be the homomorphism defined by $\varphi(x)=(1,i)$ and $\varphi(r)=(r,r)$ for r in $\mathbb{R}$. Determine the kernel and the image of φ.

解答

题目翻译: 设 $\varphi : \mathbb{R}[x] \to \mathbb{C}\times\mathbb{C}$ 是同态, 满足 $\varphi(x)=(1,i)$, 且对 $r\in\mathbb{R}$ 有 $\varphi(r)=(r,r)$. 求 φ 的核与像.
解答: 对 $f(x)=\sum_j a_j x^j$ ($a_j\in\mathbb{R}$),

$$\varphi(f)=\Big(\sum_j a_j,\ \sum_j a_j i^j\Big)=(f(1),\ f(i)).$$

核: $f\in\ker$ 当且仅当 $f(1)=0$ 且 $f(i)=0$. 因 f 是实系数多项式, $f(i)=0$ 当且仅当 $f(-i)=0$ (取共轭). 故 f 同时被 $x-1$, $x-i$, $x+i$ 整除, 即被

$$(x-1)(x-i)(x+i)=(x-1)(x^2+1)=x^3-x^2+x-1$$

整除. 所以 $\ker=(x^3-x^2+x-1)$.
像: 对任意 $(u,v)\in\mathbb{R}\times\mathbb{C}$, 写 $v=a+bi$. 取三个数据点 $(1,u)$, $(i,a+bi)$, $(-i,a-bi)$, 它们关于共轭不变, 故过这三点的 Lagrange 插值多项式 $f\in\mathbb{R}[x]$ 满足 $f(1)=u$, $f(i)=v$. 因此 $\operatorname{Im}\varphi=\mathbb{R}\times\mathbb{C}$. 由同态基本定理,

$$\mathbb{R}[x]/(x^3-x^2+x-1)\cong\mathbb{R}\times\mathbb{C}.$$

习题 6.5

Suppose we adjoin an element α satisfying the relation $\alpha^2=1$ to the real numbers $\mathbb{R}$. Prove that the resulting ring is isomorphic to the product $\mathbb{R}\times\mathbb{R}$.

解答

题目翻译: 设向实数域 $\mathbb{R}$ 添加满足 $\alpha^2 = 1$ 的元素 α. 证明所得环同构于乘积环 $\mathbb{R} \times \mathbb{R}$.
解答: 所得环是 $R' = \mathbb{R}[x]/(x^2 - 1)$. 因 $x^2 - 1 = (x - 1)(x + 1)$, 且 $x - 1$ 与 $x + 1$ 在 $\mathbb{R}[x]$ 中互素 ($(x + 1) - (x - 1) = 2$ 是单位), 由中国剩余定理 (对互素理想),

$$R' \cong \mathbb{R}[x]/(x - 1) \times \mathbb{R}[x]/(x + 1) \cong \mathbb{R} \times \mathbb{R}.$$

也可显式写同构: $\Phi(f \bmod (x^2 - 1)) = (f(1), f(-1))$. 它良定义且保持运算. 满: 对 $(a, b) \in \mathbb{R} \times \mathbb{R}$, 一次多项式 $f(x) = \frac{a-b}{2}x + \frac{a+b}{2}$ 满足 $f(1) = a$, $f(-1) = b$. 单: 若 $f(1) = f(-1) = 0$, 则 $x - 1 \mid f$ 且 $x + 1 \mid f$, 互素故 $(x - 1)(x + 1) = x^2 - 1 \mid f$, 即 f 在核中. 所以 Φ 是同构, 对应 $\alpha \mapsto (1, -1)$.

习题 7.1

Prove that a domain of finite order is a field.

解答

题目翻译: 证明: 有限阶的整环是域.
解答: 设 R 是有限整环, 取非零元 $a \in R$, 考虑左乘映射

$$\mu_a : R \to R, \qquad x \mapsto ax.$$

若 $\mu_a(x) = \mu_a(y)$, 即 $ax = ay$, 则 $a(x - y) = 0$; 因 R 是整环, 无零因子且 $a \neq 0$, 得 $x - y = 0$, 故 μ_a 是单射. 有限集合上的自映射单射必为满射, 于是存在 $b \in R$ 使 $\mu_a(b) = ab = 1$. 所以每个非零元都可逆, R 是域.

习题 7.2

Let R be a domain. Prove that the polynomial ring $R[x]$ is a domain, and identify the units in $R[x]$.

解答

题目翻译: 设 R 是整环. 证明多项式环 $R[x]$ 是整环, 并确定 $R[x]$ 中的单位.
解答: 设 $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j$ 均为非零多项式, 最高次系数 $a_m \neq 0$, $b_n \neq 0$. 乘积 fg 的最高次项系数为 $a_m b_n$; 因 R 无零因子, $a_m b_n \neq 0$, 故 $fg \neq 0$. 所以 $R[x]$ 无零因子, 是整环 (交换性与单位元 1 显然).
若 $fg = 1$, 则 $\deg f + \deg g = \deg(fg) = 0$, 故 $\deg f = \deg g = 0$, f 与 g 都是常数且互为逆. 所以 $R[x]$ 的单位恰为 R 中可逆的常数, 即 $R[x]^\times = R^\times$.

习题 8.1

Which principal ideals in $\mathbb{Z}[x]$ are maximal ideals?

解答

题目翻译:$\mathbb{Z}[x]$ 中哪些主理想是极大理想?

解答: 结论: 没有. 设 (f) 是 $\mathbb{Z}[x]$ 的极大理想, 分两种情形.

若 $\deg f = 0$, 即 $f = c$, $|c| \geq 2$ ($c = \pm 1$ 时 $(f) = \mathbb{Z}[x]$ 不是真理想). 则 $\mathbb{Z}[x]/(c) \cong (\mathbb{Z}/c\mathbb{Z})[x]$; 即使 c 是素数, 商为 $\mathbb{F}_p[x]$, 其中 x 不可逆, 不是域. 故常数生成元不可能.

若 $\deg f \geq 1$, 假设 $K = \mathbb{Z}[x]/(f)$ 是域. 设 K 的特征为素数 p, 则 $p \in \ker(\mathbb{Z} \to K) = (f)$, 即 $p = f \cdot g$; 因 $\deg f \geq 1$, 必须有 $\deg g = 0$, 于是 f 是常数, 矛盾. 所以 K 的特征为 0, $\mathbb{Z} \hookrightarrow K$, 记 $y = \bar{x}$, 则 y 满足 $f(y) = 0$, 是 $\mathbb{Q}$ 上代数元, $K = \mathbb{Z}[y]$ 含于数域 $\mathbb{Q}(y)$. 取一个不整除 f 的任一非常数项系数的素数 p (这样的 p 有无穷多个), 则 $\bar{f}$ 在 $\mathbb{F}_p[x]$ 中次数仍 ≥ 1. 若 $1/p \in K$, 则存在 $g \in \mathbb{Z}[x]$ 使 $pg(y) = 1$, 即 $1 - pg(x) \in (f)$, 即 $1 - pg(x) = f(x)h(x)$. 模 p 得 $\bar{1} = \bar{f}\bar{h}$ 在 $\mathbb{F}_p[x]$ 中, 与 $\deg \bar{f} \geq 1$ 矛盾 (域上多项式环中非平凡乘积次数至少为 1). 故 $1/p \notin K$, 与 K 是域矛盾.

综上, $\mathbb{Z}[x]$ 没有由单个元素生成的极大理想; 其极大理想都形如 $(p, f(x))$ (p 素数, $\bar{f}$ 在 $\mathbb{F}_p[x]$ 中不可约), 需要两个生成元.

习题 8.2

Determine the maximal ideals of each of the following rings: (a) $\mathbb{R} \times \mathbb{R}$, (b) $\mathbb{R}[x]/(x^2)$, (c) $\mathbb{R}[x]/(x^2 - 3x + 2)$, (d) $\mathbb{R}[x]/(x^2 + x + 1)$.

解答

题目翻译: 求下列各环的极大理想: (a) $\mathbb{R} \times \mathbb{R}$; (b) $\mathbb{R}[x]/(x^2)$; (c) $\mathbb{R}[x]/(x^2 - 3x + 2)$; (d) $\mathbb{R}[x]/(x^2 + x + 1)$.

解答:(a) $\mathbb{R}$ 是域, 其理想只有 (0) 与 $\mathbb{R}$. 乘积环 $\mathbb{R} \times \mathbb{R}$ 的每个理想都形如 $I \times J$ (I, J 为 $\mathbb{R}$ 的理想), 故非零真理想为 $\mathbb{R} \times \{0\}$ 与 $\{0\} \times \mathbb{R}$. 它们都是极大的, 因为商分别为 $\{0\} \times \mathbb{R} \cong \mathbb{R}$ 与 $\mathbb{R} \times \{0\} \cong \mathbb{R}$, 是域.

(b) 记 $S = \mathbb{R}[x]/(x^2)$, 元素为 $a + b\bar{x}$. $a + b\bar{x}$ 可逆当且仅当 $a \neq 0$ (逆为 $a^{-1} - a^{-2}b\,\bar{x}$). 故非单位恰为 $a = 0$ 的元素, 即理想 $(\bar{x}) = (x)/(x^2)$. 一切真理想都被 $(\bar{x})$ 包含, 所以 $(\bar{x})$ 是唯一极大理想, 商 $S/(\bar{x}) \cong \mathbb{R}$ 是域. 该环是局部环.

(c) $x^2 - 3x + 2 = (x - 1)(x - 2)$, 且 $x - 1$ 与 $x - 2$ 互素 ($(x - 2) - (x - 1) = -1$ 是单位). 由中国剩余定理, $\mathbb{R}[x]/((x - 1)(x - 2)) \cong \mathbb{R} \times \mathbb{R}$. 由 (a), 极大理想为 $\mathbb{R} \times \{0\}$ 与 $\{0\} \times \mathbb{R}$, 在商环中对应为 $x \bar{-} 1$ 生成的理想 $(x \bar{-} 1)$ 与 $x \bar{-} 2$ 生成的理想 $(x \bar{-} 2)$.

(d) $x^2 + x + 1$ 在 $\mathbb{R}$ 上不可约 (判别式 $-3 < 0$), 故 $\mathbb{R}[x]/(x^2 + x + 1)$ 是域 (同构于 $\mathbb{C}$). 域的极大理想只有零理想, 故唯一极大理想为 (0).

习题 12.4

Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly. Is G/H isomorphic to G?

解答

题目翻译: 设 $H = \{\pm 1, \pm i\}$ 是 $G = \mathbb{C}^\times$ (非零复数乘法群) 的四次单位根子群. 显式描述 H 在 G 中的陪集. G/H 是否同构于 G?

解答: 每个 $z = re^{i\theta}$ $(r > 0)$ 的陪集为

$$zH = \{\pm re^{i\theta},\ \pm i\, re^{i\theta}\},$$

即把 z 相继旋转 90° 得到的四个点. 两个元素 z, w 同属一个陪集当且仅当 $z/w \in H$, 即 $|z| = |w|$ 且幅角差为 $\pi/2$ 的整数倍. 因此陪集由 $(r, \theta \bmod \pi/2)$ 唯一确定; 每个陪集有唯一代表元 $re^{i\theta}$, $\theta \in [0, \pi/2)$, 陪集全体与 $\mathbb{R}_{>0} \times [0, \pi/2)$ 一一对应.

$G/H \cong G$. 事实上映射 $z \mapsto z^4$ 是 G 到 G 的满同态 ($\mathbb{C}^\times$ 中每个元素都有四次根), 其核为 $\{z : z^4 = 1\} = \{\pm 1, \pm i\} = H$. 由群同态基本定理, $G/H \cong G$.

习题 1.5

Determine all subrings of $\mathbb{R}$ that are discrete sets.

解答

题目翻译: 确定 $\mathbb{R}$ 的所有离散子环.

解答: 先看加法结构. $\mathbb{R}$ 的离散加法子群只有 $c\mathbb{Z}$ $(c \geq 0)$: 若非零, 取 $a = \inf(G \cap \mathbb{R}_{>0}) > 0$ (离散性保证 $a \in G$), 则对 $g \in G$, 写 $g = ka + r$, $0 \leq r < a$, 由 $r = g - ka \in G$ 得 $r = 0$, 故 $G = a\mathbb{Z}$.

设 $S = c\mathbb{Z}$ 是子环, $c > 0$. 乘法封闭要求 $(mc)(nc) = mnc^2 \in c\mathbb{Z}$ 对一切 $m, n \in \mathbb{Z}$, 等价于 $c^2 \in c\mathbb{Z}$, 即 $c \in \mathbb{Z}_{>0}$. 故候选为 $n\mathbb{Z}$, $n \geq 1$, 以及 $\{0\}$. 按 Artin 教材约定, 子环必须含有单位元 1: 此时只有 $n = 1$, 答案是 $\mathbb{Z}$; 零环 $\{0\}$ 不含 1, 但若放宽约定, 它也是离散的 (对减法与乘法封闭). 因此: 含单位元的离散子环只有 $\mathbb{Z}$; 若允许零环, 则还有 $\{0\}$. ($n\mathbb{Z}$, $n \geq 2$, 因不含 1 而不属于含单位元的子环.)

习题 1.8

Determine the units in: (a) $\mathbb{Z}/12\mathbb{Z}$, (b) $\mathbb{Z}/8\mathbb{Z}$, (c) $\mathbb{Z}/n\mathbb{Z}$.

解答

题目翻译: 求下列环中的单位: (a) $\mathbb{Z}/12\mathbb{Z}$; (b) $\mathbb{Z}/8\mathbb{Z}$; (c) $\mathbb{Z}/n\mathbb{Z}$.

解答: 一般结论: $\bar{k}$ 在 $\mathbb{Z}/n\mathbb{Z}$ 中可逆当且仅当存在 m 使 $km - nq = 1$ 对某整数 q, 由 Bezout 定理, 这等价于 $\gcd(k, n) = 1$. (a) 与 12 互素的剩余类: $1, 5, 7, 11$. (b) 与 8 互

素的剩余类: $1,3,5,7$. (c) 单位集为 $\{\bar{k} : \gcd(k,n)=1\}$, 共有 $\varphi(n)$ 个 (φ 为 Euler 函数), 即 $(\mathbb{Z}/n\mathbb{Z})^\times$ 是 $\varphi(n)$ 阶乘法群.

习题 2.2

Let F be a field. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with a_i in F, forms a ring that is often denoted by $F[\![t]\!]$. Prove that $F[\![t]\!]$ is a ring, and determine the units in this ring.

解答

题目翻译: 设 F 是域. 形如 $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$ ($a_i \in F$) 的形式幂级数全体构成环 $F[\![t]\!]$. 证明 $F[\![t]\!]$ 是环, 并求该环的单位.

解答: 加法逐项定义, 零元为 $0 + 0t + \cdots$, 负元逐项取负, $F[\![t]\!]$ 成为加法 Abel 群. 乘法定义为

$$\Big(\sum_i a_i t^i\Big)\Big(\sum_j b_j t^j\Big) = \sum_k \Big(\sum_{i+j=k} a_i b_j\Big) t^k,$$

每个 t^k 的系数是有限和, 故良定义. 结合律与分配律由系数比较归结为 F 中的运算律, 单位元为 $1 = 1 + 0t + \cdots$. 故 $F[\![t]\!]$ 是交换幺环.

单位: 若 $f = \sum_i a_i t^i$ 可逆, 则 $fg = 1$ 的常数项 $a_0 b_0 = 1$, 故 $a_0 \neq 0$. 反之设 $a_0 \neq 0$, 递归求逆: 令 $b_0 = a_0^{-1}$, 对 $k \geq 1$ 由 $\sum_{i=0}^{k} a_i b_{k-i} = 0$ 解得

$$b_k = -a_0^{-1}\Big(\sum_{i=1}^{k} a_i b_{k-i}\Big),$$

故 $g = \sum_j b_j t^j$ 满足 $fg = 1$. 所以 $F[\![t]\!]$ 的单位恰为常数项非零的幂级数.

习题 3.6

An automorphism of a ring R is an isomorphism from R to itself. Let R be a ring, and let $f(y)$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x,y] \to R[x,y]$ defined by $x \mapsto x + f(y)$, $y \mapsto y$ is an automorphism of $R[x,y]$.

解答

题目翻译: 环 R 的自同构是 R 到自身的同构. 设 R 是环, $f(y)$ 是系数在 R 中的一元多项式. 证明映射 $R[x,y] \to R[x,y]$, $x \mapsto x + f(y)$, $y \mapsto y$ 是 $R[x,y]$ 的自同构.

解答: 由多项式环的代入原理 (universal property), 指定两个变元的像即唯一确定环同态

$$\varphi : R[x,y] \to R[x,y], \qquad \varphi(x) = x + f(y),\ \varphi(y) = y,\ \varphi \text{ 在} R \text{ 上恒等}.$$

构造 $\psi : R[x,y] \to R[x,y]$, $\psi(x) = x - f(y)$, $\psi(y) = y$. 计算复合:

$$\psi(\varphi(x)) = \psi(x + f(y)) = \psi(x) + f(\psi(y)) = (x - f(y)) + f(y) = x,$$

且 $\psi(\varphi(y)) = \psi(y) = y$; 同理 $\varphi \circ \psi$ 在 x, y 上也是恒等. 因为 x, y 生成 $R[x,y]$ (作为 R-代数), 故 $\psi \circ \varphi = \varphi \circ \psi = \mathrm{id}$, φ 是双射. 所以 φ 是自同构. (直观上这是把变元 x 平移 $f(y)$ 的替换, 其逆为反平移.)

习题 3.7

Determine the automorphisms of the polynomial ring $\mathbb{Z}[x]$ (see Exercise 3.6).

解答

题目翻译: 求多项式环 $\mathbb{Z}[x]$ 的全部自同构 (参见习题 3.6).
解答: 环同态把 1 映到 1, 故自同构在 $\mathbb{Z}$ 上恒等, 因而由 $\sigma(x) = g(x)$ 完全决定. 因 σ 是满射, 存在 $h \in \mathbb{Z}[x]$ 使 $\sigma(h) = x$, 即 $h(g(x)) = x$. 在整环 $\mathbb{Z}[x]$ 中 $\deg(h(g)) = \deg h \cdot \deg g = \deg x = 1$, 故 $\deg g = \deg h = 1$. 写 $g(x) = ax + b$, $a \neq 0$. 逆映射须把 x 送到 $a^{-1}(x - b)$, 它为整系数多项式当且仅当 $a = \pm 1$. 直接验证: $x \mapsto x + b$ 的逆是 $x \mapsto x - b$; $x \mapsto -x + b$ 的逆是它自身. 故全部自同构为

$$x \mapsto x + b \quad \text{与} \quad x \mapsto -x + b, \qquad b \in \mathbb{Z}.$$

习题 3.8

Let R be a ring of prime characteristic p. Prove that the map $R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism. (It is called the Frobenius map.)

解答

题目翻译: 设 R 是素数特征 p 的环. 证明映射 $R \to R$, $x \mapsto x^p$ 是环同态 (称为 Frobenius 映射).
解答: 按 Artin 环论部分, R 是交换环. 乘法: $(ab)^p = a^p b^p$ (交换律); 单位元: $1^p = 1$. 加法: 由二项式定理,

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j.$$

当 $1 \le j \le p-1$ 时, $\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}$ 是整数; 因 p 是素数, 分子含因子 p 而 $j!$ 不含, 故该整数被 p 整除. 特征 p 使 $p \cdot c = 0$, 所以中间各项全为零, 得

$$(a+b)^p = a^p + b^p.$$

因此 $x \mapsto x^p$ 保持加法和乘法, 是环同态.

习题 3.10

Determine all ideals of the ring $F[\![t]\!]$ of formal power series with coefficients in a field F (see Exercise 2.2).

解答

题目翻译: 求域 F 上形式幂级数环 $F[\![t]\!]$ 的全部理想 (参见习题 2.2).
解答: 对非零幂级数 $f=\sum_i a_i t^i$, 定义阶 $\operatorname{ord}(f)$ 为最小使 $a_i\neq 0$ 的指数 i. 若 $f\neq 0$, 记 $m=\operatorname{ord}(f)$, 则 $f=t^m u$ 其中 u 的常数项 $a_m\neq 0$, 由习题 2.2 知 u 可逆.
结论: $F[\![t]\!]$ 的理想只有 (0) 与 (t^n), $n\geq 1$. 证明: 设 I 是非零理想, 取 $f\in I$ 使 $m=\operatorname{ord}(f)$ 在所有非零元中最小. 由 $f=t^m u$ 且 u 可逆得 $t^m=fu^{-1}\in I$, 故 $(t^m)\subseteq I$. 反之, 对任意 $g\in I$, $\operatorname{ord}(g)\geq m$, 写 $g=t^m v$ $(v\in F[\![t]\!])$, 故 $g\in(t^m)$, 即 $I\subseteq(t^m)$. 所以 $I=(t^m)$. 理想链为

$$F[\![t]\!]=(t^0)\supsetneq(t)\supsetneq(t^2)\supsetneq\cdots,$$

其中 (t) 是唯一极大理想, 且 $\bigcap_{n\geq 1}(t^n)=(0)$.

习题 3.13

Let I and J be ideals of a ring R. Prove that the intersection $I\cap J$ is an ideal. Show by example that the set of products $\{xy\mid x\in I, y\in J\}$ need not be an ideal, but that the set of finite sums $\sum_\nu x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the product ideal, and is denoted by IJ. Is there a relation between IJ and $I\cap J$?

解答

题目翻译: 设 I, J 是环 R 的理想. 证明 $I\cap J$ 是理想. 举例说明乘积集 $\{xy\mid x\in I, y\in J\}$ 不必是理想, 但有限和 $\sum_\nu x_\nu y_\nu$ $(x_\nu\in I,\ y_\nu\in J)$ 的集合是理想, 称为乘积理想, 记作 IJ. IJ 与 $I\cap J$ 有何关系?
解答: $I\cap J$ 是理想: $0\in I\cap J$; 对 $a,b\in I\cap J$, $a-b\in I$ 且 $a-b\in J$, 故 $a-b\in I\cap J$; 对 $r\in R$, $ra, ar\in I$ 且 $\in J$. 验证完毕.
乘积集不封闭的例子: 取 $R=\mathbb{R}[x,y]$, $I=J=(x,y)$. 则 $x^2=x\cdot x$ 与 $y^2=y\cdot y$ 都在乘积集中. 但 x^2+y^2 不是单个乘积: 若 $x^2+y^2=(xf+yg)(xu+yv)$, 比较 x^2, xy, y^2 的系数得 $fu=1$, $fv+gu=0$, $gv=1$. 由 $fu=1$ 知 f,u 是 $\mathbb{R}[x,y]$ 中的单位, 即为非零常数; 同理 g,v 是非零常数. 于是 $fv+gu=2cd\neq 0$ (特征 0), 矛盾. 所以 x^2+y^2 不在乘积集中, 乘积集对加法不封闭, 不是理想.
IJ 是理想: 非空 $(0=0\cdot 0)$; 两个有限和相减仍是有限和, 故对减法封闭; 对 $r\in R$,

$$r\Big(\sum_\nu x_\nu y_\nu\Big)=\sum_\nu (rx_\nu)y_\nu\in IJ,$$

同理右侧吸收成立. 故 IJ 是理想.
关系: 每个乘积 $x_\nu y_\nu$ 因 $y_\nu \in R$, $x_\nu \in I$ 而属于 I, 又因 $x_\nu \in R$ 属于 J, 故 $IJ \subseteq I \cap J$. 包含可以严格, 如 $R = F[x]$, $I = J = (x)$, 则 $IJ = (x^2) \subsetneq (x) = I \cap J$. 当 I 与 J 互素 (即 $I + J = R$) 时 $IJ = I \cap J$, 见习题 6.8(a).

习题 4.3

Identify the following rings: (a) $\mathbb{Z}[x]/(x^2-3, 2x+4)$, (b) $\mathbb{Z}[i]/(2+i)$, (c) $\mathbb{Z}[x]/(6, 2x-1)$, (d) $\mathbb{Z}[x]/(2x^2-4, 4x-5)$, (e) $\mathbb{Z}[x]/(x^2+3, 5)$.

解答

题目翻译: 识别下列环: (a) $\mathbb{Z}[x]/(x^2-3, 2x+4)$; (b) $\mathbb{Z}[i]/(2+i)$; (c) $\mathbb{Z}[x]/(6, 2x-1)$; (d) $\mathbb{Z}[x]/(2x^2-4, 4x-5)$; (e) $\mathbb{Z}[x]/(x^2+3, 5)$.
解答:(a) 记 $S = \mathbb{Z}[x]/(x^2-3, 2x+4)$. 由 $2x = -4$ 两边乘 x: $2x^2 = -4x$; 用 $x^2 = 3$ 得 $6 = -4x$, 即 $4x = -6$. 另一方面 $4x = 2(2x) = -8$, 故 $-8 = -6$, 得 $2 = 0$. 于是特征 2, 关系 $2x + 4 = 4 = 0$ 自动成立, $x^2 = 3 = 1$ (模 2). 所以 $S \cong \mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[x]/((x+1)^2)$. 令 $\varepsilon = x + 1$, 得 $S \cong \mathbb{F}_2[\varepsilon]/(\varepsilon^2)$, 含 4 个元素, 是含非零零因子 ($\varepsilon^2 = 0$) 的局部环.
(b) 在 $\mathbb{Z}[i]/(2+i)$ 中 $i = -2$, 于是 $-1 = i^2 = 4$, 得 $5 = 0$. 商环元素都被 5 控制 (也可由范 $N(2+i) = 5$ 知商环含 5 个元素), 故 $\mathbb{Z}[i]/(2+i) \cong \mathbb{F}_5$.
(c) 由 $2x = 1$ 得 $6x = 3$, 而 $6 = 0$, 故 $3 = 0$, 特征 3. 在 $\mathbb{F}_3$ 中 $2x = 1$ 给出 $x = 2$ (因 $2^{-1} = 2$). 所以 $\mathbb{Z}[x]/(6, 2x-1) \cong \mathbb{F}_3$, 其中 $\bar{x} = 2$.
(d) 由 $4x = 5$ 两边乘 x: $4x^2 = 5x$; 又 $2x^2 = 4$ 乘 2 得 $4x^2 = 8$, 故 $5x = 8$. 把 $4x = 5$ 乘 5 得 $20x = 25$, 把 $5x = 8$ 乘 4 得 $20x = 32$, 相减得 $7 = 0$. 在 $\mathbb{F}_7$ 中 $4x = 5$, 而 $4^{-1} = 2$, 故 $x = 10 = 3$; 且 $2x^2 - 4 = 2 \cdot 9 - 4 = 18 - 4 = 14 = 0$ (模 7) 成立. 所以 $\mathbb{Z}[x]/(2x^2-4, 4x-5) \cong \mathbb{F}_7$.
(e) $\mathbb{Z}[x]/(x^2+3, 5) = \mathbb{F}_5[x]/(x^2+3) = \mathbb{F}_5[x]/(x^2-2)$ (因 $3 \equiv -2 \pmod 5$). $\mathbb{F}_5$ 中的平方是 $0, 1, 4$, 2 不是平方, 故 $x^2 - 2$ 在 $\mathbb{F}_5$ 上不可约, 商是含 $5^2 = 25$ 个元素的域, 即 $\mathbb{F}_{25}$.

习题 5.4

Determine the structure of the ring R' obtained from $\mathbb{Z}$ by adjoining an element α satisfying each set of relations.
(a) $2\alpha = 6$, $6\alpha = 15$,
(b) $2\alpha - 6 = 0$, $\alpha - 10 = 0$,
(c) $\alpha^3 + \alpha^2 + 1 = 0$, $\alpha^2 + \alpha = 0$.

解答

题目翻译: 确定由 $\mathbb{Z}$ 添加元素 α, 满足下列各组关系的环 R' 的结构.
解答:(a) $R' = \mathbb{Z}[x]/(2x-6, 6x-15)$. 计算

$$(6x-15) - 3(2x-6) = 3,$$

故 3 在理想中, 商环中 $3 = 0$, 特征 3. 此时 $2x - 6 = 2x = 0$; 2 在 $\mathbb{F}_3$ 中可逆, 故 $x = 0$. 所以 $R' \cong \mathbb{F}_3$, 其中 $\alpha = 0$.
(b) $R' = \mathbb{Z}[x]/(2x-6, x-10)$. 由 $x = 10$ 代入 $2x - 6 = 14$, 故 $14 = 0$; 且 $2x - 6 = 2(x-10) + 14$, 所以 $(2x-6, x-10) = (14, x-10)$. 于是

$$R' \cong \mathbb{Z}[x]/(14, x-10) \cong \mathbb{Z}/14\mathbb{Z},$$

其中 $\alpha = 10$ (模 14).
(c) $R' = \mathbb{Z}[x]/(x^3+x^2+1, x^2+x)$. 由 $x^2+x = 0$ 得 $x^2 = -x$, 于是 $x^3 = x \cdot x^2 = -x^2 = x$. 代入第一式:

$$x^3 + x^2 + 1 = x + (-x) + 1 = 1,$$

故 $1 = 0$ 在商环中. 所以 R' 是零环.

习题 5.5

Are there fields F such that the rings $F[x]/(x^2)$ and $F[x]/(x^2-1)$ are isomorphic?

解答

题目翻译: 是否存在域 F, 使 $F[x]/(x^2)$ 与 $F[x]/(x^2-1)$ 同构?
解答: 存在, 恰为特征 2 的域. $F[x]/(x^2)$ 中有非零零因子 $\bar{x}$, 且 $\bar{x}^2 = 0$ (幂零元). 若 $\operatorname{char} F \neq 2$, 则 $x^2 - 1 = (x-1)(x+1)$, 且 $x-1$ 与 $x+1$ 互素 ($(x+1) - (x-1) = 2$ 是单位), 由中国剩余定理

$$F[x]/(x^2-1) \cong F[x]/(x-1) \times F[x]/(x+1) \cong F \times F.$$

域上的乘积环无幂零元 (因 $(\alpha, \beta)^n = 0 \Rightarrow \alpha^n = \beta^n = 0 \Rightarrow \alpha = \beta = 0$), 故不与 $F[x]/(x^2)$ 同构. 若 $\operatorname{char} F = 2$, 则 $x^2 - 1 = x^2 + 1 = (x+1)^2$, 作替换 $u = x + 1$ 得

$$F[x]/(x^2-1) = F[x]/((x+1)^2) \cong F[u]/(u^2) \cong F[x]/(x^2).$$

答案: 有, 当且仅当 $\operatorname{char} F = 2$.

习题 5.6

Let a be an element of a ring R, and let R' be the ring $R[x]/(ax-1)$ obtained by adjoining an inverse of a to R. Let α denote the residue of x (the inverse of a in R').
(a) Show that every element β of R' can be written in the form $\beta = \alpha^k b$, with b in R.
(b) Prove that the kernel of the map $R \to R'$ is the set of elements b of R such that $a^n b = 0$ for some $n > 0$.
(c) Prove that R' is the zero ring if and only if a is nilpotent.

解答

题目翻译: 设 a 是环 R 的元素, $R' = R[x]/(ax-1)$ 是在 R 中添加 a 的逆所得环, α 是 x 的剩余类 (a 在 R' 中的逆). (a) 证明 R' 的每个元素 β 都可写成 $\beta = \alpha^k b$, $b \in R$. (b) 证明映射 $R \to R'$ 的核是 $\{b \in R : a^n b = 0 \text{ 对某} n > 0\}$. (c) 证明 R' 是零环当且仅当 a 幂零.

解答:(a) R' 的元素形如 $\beta = \sum_{i=0}^{n} r_i \alpha^i$, $r_i \in R$. 因 $a\alpha = 1$, 有 $\alpha^{-1} = a$, 故对 $i \le n$,

$$\alpha^i = \alpha^n \alpha^{i-n} = \alpha^n a^{n-i}.$$

于是 $\beta = \alpha^n \sum_{i=0}^{n} r_i a^{n-i}$. 取 $b = \sum_{i=0}^{n} r_i a^{n-i} \in R$ 即可.
(b) b 在核中当且仅当 $b = 0$ 在 R' 中. 先证充分: 若 $a^n b = 0$, 则在 R' 中

$$b = (a\alpha)^n b = a^n \alpha^n b = \alpha^n (a^n b) = 0.$$

再证必要: 设 $b \in (ax-1)$, 写 $b = (ax-1)(c_0 + c_1 x + \cdots + c_m x^m)$, 展开并比较系数: 常数项 $b = -c_0$; x 的系数 $ac_0 - c_1 = 0$; …; x^m 的系数 $ac_{m-1} - c_m = 0$; x^{m+1} 的系数 $ac_m = 0$. 依次解得 $c_j = -a^j b$, 最后由 $ac_m = 0$ 得 $a^{m+1} b = 0$. 故 b 属于所述集合.
(c) R' 是零环当且仅当 $1 = 0$ 在 R' 中, 当且仅当 1 在映射 $R \to R'$ 的核中. 由 (b), 这等价于存在 $n > 0$ 使 $a^n \cdot 1 = 0$, 即 a 幂零.

习题 6.6

Describe the ring obtained from the product ring $\mathbb{R} \times \mathbb{R}$ by inverting the element $(2, 0)$.

解答

题目翻译: 描述由乘积环 $\mathbb{R} \times \mathbb{R}$ 对元素 $(2,0)$ 求逆所得的环.
解答: 该环是 $R' = (\mathbb{R} \times \mathbb{R})[x]/((2,0)x - (1,1))$. 生成关系 $(2,0)x = (1,1)$ 逐分量看: 第一分量 $2x_1 = 1$, 第二分量 $0 \cdot x_2 = 1$. 第二式在 $\mathbb{R}$ 中迫使 $0 = 1$, 故第二个分量所在的环被压成零环; 第一式给出 $x_1 = \frac{1}{2} \in \mathbb{R}$, 而 2 在 $\mathbb{R}$ 中本就可逆, 第一分量不变. 因此

$$R' \cong \mathbb{R} \times \{0\} \cong \mathbb{R}.$$

(等价地, 这是对乘性集 $S=\{(2^k,0^k):k\geq 0\}$ 的局部化: 第二分量的乘性集含 0, 局部化为零环; 第一分量局部化不改变, 因为 2 已是 $\mathbb{R}$ 中的单位.)

习题 6.2

Is $\mathbb{Z}/(6)$ isomorphic to the product ring $\mathbb{Z}/(2)\times\mathbb{Z}/(3)$? Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$?

解答

题目翻译:$\mathbb{Z}/(6)$ 是否同构于乘积环 $\mathbb{Z}/(2)\times\mathbb{Z}/(3)$? $\mathbb{Z}/(8)$ 是否同构于 $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$?
解答: 第一个是. 映射

$$\mathbb{Z}/(6)\to\mathbb{Z}/(2)\times\mathbb{Z}/(3),\qquad \bar{a}\mapsto(\bar{a},\bar{a})$$

是环同态. 核: a 同时被 2 和 3 整除当且仅当 a 被 6 整除 (因 2, 3 互素), 故单; 两边各 6 个元素, 单射即双射. 此即整数情形的中国剩余定理.
第二个否. 作为加法群, $\mathbb{Z}/(8)$ 是 8 阶循环群, 有 8 阶元 $\bar{1}$; 而 $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$ 中每个元素的阶整除 $\operatorname{lcm}(2,4)=4$, 无 8 阶元. 环同构必为加法群同构, 故两环不同构. (另一标志: $\mathbb{Z}/(8)$ 只有一个极大理想 $(\bar{2})$, 而 $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$ 有两个极大理想.)

习题 6.8

Let I and J be ideals of a ring R such that $I+J=R$.
(a) Prove that $IJ=I\cap J$.
(b) Prove the Chinese Remainder Theorem: For any pair a, b of elements of R, there is an element x such that $x\equiv a \pmod I$ and $x\equiv b \pmod J$.
(c) Prove that if $IJ=0$, then R is isomorphic to the product ring $(R/I)\times(R/J)$.
(d) Describe the idempotents corresponding to the product decomposition in (c).

解答

题目翻译: 设 I, J 是环 R 的理想且 $I+J=R$. (a) 证明 $IJ=I\cap J$. (b) 证明中国剩余定理: 对任意 $a,b\in R$, 存在 x 使 $x\equiv a \pmod I$ 且 $x\equiv b \pmod J$. (c) 证明若 $IJ=0$, 则 $R\cong(R/I)\times(R/J)$. (d) 描述 (c) 中乘积分解对应的幂等元.
解答: 由 $I+J=R$, 存在 $i_0\in I$, $j_0\in J$ 使 $i_0+j_0=1$.
(a) 习题 3.13 已证 $IJ\subseteq I\cap J$. 反方向: 对 $c\in I\cap J$,

$$c=c\cdot 1=c(i_0+j_0)=ci_0+cj_0.$$

其中 $ci_0\in JI\subseteq IJ$ (因 $c\in J$, $i_0\in I$), $cj_0\in IJ$ (因 $c\in I$, $j_0\in J$), 故 $c\in IJ$. 所以 $IJ=I\cap J$.

(b) 令 $x = bi_0 + aj_0$. 则

$$x - a = bi_0 + aj_0 - a = bi_0 + a(j_0 - 1) = bi_0 - ai_0 = (b-a)i_0 \in I,$$

故 $x \equiv a \pmod{I}$; 又

$$x - b = b(i_0 - 1) + aj_0 = -bj_0 + aj_0 = (a-b)j_0 \in J,$$

故 $x \equiv b \pmod{J}$.
(c) 定义环同态

$$\varphi : R \to (R/I) \times (R/J), \qquad r \mapsto (r+I,\, r+J).$$

核: $r \in \ker\varphi \iff r \in I \cap J = IJ = 0$, 故 φ 单. 满: 由 (b), 对任意 $(a+I, b+J)$ 存在 x 同时满足 $x \equiv a \pmod{I}$, $x \equiv b \pmod{J}$, 于是 $\varphi(x) = (a+I, b+J)$. 所以 φ 是同构.
(d) 单位分解 $1 = i_0 + j_0$ 给出两个幂等元 $e_1 = j_0$, $e_2 = i_0$: 因

$$\varphi(j_0) = (j_0 + I,\ j_0 + J) = (1 + I,\ 0 + J), \qquad \varphi(i_0) = (0 + I,\ 1 + J)$$

(第一分量用 $j_0 = 1 - i_0$, $i_0 \in I$; 第二分量用 $j_0 \in J$). 它们满足 $e_1 + e_2 = 1$, $e_1 e_2 = j_0 i_0 \in IJ = 0$, 且由 φ 的单射性从分量的幂等性推出 $e_1^2 = e_1$, $e_2^2 = e_2$. 乘积分解中 e_1 对应因子 R/I, e_2 对应因子 R/J.

习题 7.4

Prove that the field of fractions of the formal power series ring $F[\![x]\!]$ over a field F can be obtained by inverting the element x. Find a neat description of the elements of that field (see Exercise 11.2.1).

解答

题目翻译: 证明域 F 上形式幂级数环 $F[\![x]\!]$ 的分式域可由对 x 求逆得到. 给出该域元素的简洁描述 (参见习题 11.2.1).
解答: 由习题 2.2, $F[\![x]\!]$ 的每个非零元 f 可唯一写成 $f = x^m u$, 其中 $m = \operatorname{ord}(f) \geq 0$, u 是单位. 于是 f 的逆为 $u^{-1}x^{-m}$, 属于在 $F[\![x]\!]$ 中添加 x 的逆所得的环 $F[\![x]\!][x^{-1}]$. 因此任意分式 f/g $(g \neq 0)$ 都等于 $fg^{-1} \in F[\![x]\!][x^{-1}]$, 分式域包含于 $F[\![x]\!][x^{-1}]$; 反之分式域显然含 x^{-1}, 故两者相等. 该域的元素形如

$$\sum_{i \geq -n} a_i x^i, \qquad n \geq 0,$$

即 Laurent 型幂级数 (负指数部分只有有限多项), 称为形式 Laurent 级数域, 记作 $F((x))$.

习题 7.5

A subset S of a domain R that is closed under multiplication and that does not contain 0 is called a multiplicative set. Given a multiplicative set S, define S-fractions to be elements of the form a/b, where b is in S. Show that the equivalence classes of S-fractions form a ring.

解答

题目翻译: 整环 R 中在乘法下封闭且不含 0 的子集 S 称为乘性集. 给定乘性集 S, 称形如 a/b ($b \in S$) 的元素为 S-分数. 证明 S-分数的等价类构成一个环.

解答: 在集合 $R \times S$ 上定义关系 $(a,b) \sim (a',b') \iff ab' = a'b$, 记 a/b 为 (a,b) 的等价类. 自反, 对称显然. 传递: 设 $(a,b) \sim (a',b')$ 且 $(a',b') \sim (a'',b'')$, 即 $ab' = a'b$, $a'b'' = a''b'$. 两式分别乘 b'' 与 b:

$$ab'b'' = a'bb'', \qquad a'b''b = a''b'b.$$

于是 $ab'b'' = a''b'b$. 因 $b' \in S$, $b' \neq 0$ (乘性集不含 0), 且 R 是整环, 消去 b' 得 $ab'' = a''b$, 即 $(a,b) \sim (a'',b'')$. 故 $\sim$ 是等价关系.

定义运算

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

因 $b,d \in S$ 且 S 乘法封闭, $bd \in S$, 分母非零, 运算良定义; 与代表元选择无关可由交叉相乘归结为 R 中的等式 (乘法同理). 各环公理由 R 的运算律继承: 加法结合, 交换, 零元 $0/1$, 负元 $-a/b$; 乘法结合, 交换, 单位元 $1/1$; 分配律成立. 故 S-分数的等价类构成一个交换环, 称为 R 对 S 的局部化, 记作 $S^{-1}R$; 映射 $r \mapsto r/1$ 是环同态 (在整环情形它是单射).

习题 8.3

Prove that the ring $\mathbb{F}_2[x]/(x^3+x+1)$ is a field, but that $\mathbb{F}_3[x]/(x^3+x+1)$ is not a field.

解答

题目翻译: 证明 $\mathbb{F}_2[x]/(x^3+x+1)$ 是域, 而 $\mathbb{F}_3[x]/(x^3+x+1)$ 不是域.

解答: 记 $f(x) = x^3+x+1$. 域上三次多项式可约当且仅当它有线性因子, 即在该域中有根.

在 $\mathbb{F}_2$ 中: $f(0) = 1$, $f(1) = 1+1+1 = 1$, 均非零, 故 f 无根, 在 $\mathbb{F}_2$ 上不可约. 因为 $\mathbb{F}_2[x]$ 是主理想整环, 域上不可约多项式生成的主理想是极大理想, 所以 $\mathbb{F}_2[x]/(f)$ 是

域; 它有 $2^3=8$ 个元素, 即 $\mathbb{F}_8$.
在 $\mathbb{F}_3$ 中: $f(1)=1+1+1=3=0$, 故 $x-1$ 整除 f. 因式分解

$$x^3+x+1=(x-1)(x^2+x+2)$$

(验证: $(x-1)(x^2+x+2)=x^3+x^2+2x-x^2-x-2=x^3+x-2=x^3+x+1$ 在 $\mathbb{F}_3$ 中). 故 (f) 不是素理想, 商环含零因子: $(\bar{x}-1)(\overline{x^2+x+2})=0$ 且两者非零. 所以 $\mathbb{F}_3[x]/(x^3+x+1)$ 不是域.

3

第三次作业

习题 1.2

Let V be an abelian group. Prove that if V has a structure of $\mathbb{Q}$-module with its given law of composition as addition, then that structure is uniquely determined.

解答

题目翻译: 设 V 是一个 Abel 群. 证明: 若 V 以给定的合成法则作为加法而带有 $\mathbb{Q}$-模结构, 则该结构是唯一确定的.
解答: 证明: 设 V 带有 $\mathbb{Q}$-模结构. 我们要证明该结构由加法群 $(V,+)$ 完全决定, 即 $\mathbb{Q}$ 在 V 上的作用唯一.
先确定整数的作用. 对正整数 n, 模公理推出 $nv=v+v+\cdots+v$ (n 项相加); 对 $n=0$, $0v=0$; 对负整数 n, $nv=(-n)(-v)$. 这些都只用到加法, 故 $\mathbb{Z}$ 在 V 上的作用唯一.
再看 $1/n$ 的作用 ($n\geq 1$). 由模公理中的结合律,

$$v=1\cdot v=\left(n\cdot\frac{1}{n}\right)v=n\cdot\left(\frac{1}{n}v\right),$$

所以 $\frac{1}{n}v$ 是满足 $nw=v$ 的元素 w. 这样的 w 唯一: 若 $nw=v=nw'$, 则 $n(w-w')=0$, 两边乘以 $\frac{1}{n}$ 得

$$w-w'=\frac{1}{n}\big(n(w-w')\big)=\frac{1}{n}\cdot 0=0,$$

即 $w=w'$. 因此 $\frac{1}{n}v$ 由 v 与加法唯一决定.
对任意 $q=\frac{a}{b}\in\mathbb{Q}$ ($a\in\mathbb{Z}$, $b\geq 1$), 有 $qv=a\left(\frac{1}{b}v\right)$, 故 q 的作用由 $\mathbb{Z}$-作用唯一决定, 进而由加法群结构唯一决定. 故 $\mathbb{Q}$-模结构唯一.

习题 1.4

A module is called simple if it is not the zero module and if it has no proper submodule.
(a) Prove that any simple R-module is isomorphic to an R-module of the form R/M, where M is a maximal ideal.
(b) Prove Schur's Lemma: Let $\varphi : S \to S'$ be a homomorphism of simple modules. Then φ is either zero, or an isomorphism.

解答

题目翻译: 一个模称为单模, 若它既不是零模又没有真子模.
(a) 证明: 任一单 R-模同构于形如 R/M 的 R-模, 其中 M 是极大理想.
(b) 证明 Schur 引理: 设 $\varphi : S \to S'$ 是单模之间的同态, 则 φ 要么是零同态, 要么是同构.
解答: (a) 设 S 是非零单 R-模. 取非零元素 $s \in S$, 定义模同态 $f : R \to S$, $r \mapsto rs$. 像 Rs 是 S 的子模, 且含 $s = 1 \cdot s \neq 0$, 故 $Rs \neq 0$. 由 S 的单性, $Rs = S$, 即 f 是满射. 第一模同构定理给出 $S \cong R/M$, 其中 $M = \ker f$ 是 R 的子模 (即理想).
由子模对应定理, R/M 的子模与 R 中包含 M 的理想一一对应. 因 $R/M \cong S$ 是单模, R/M 无非零真子模, 故不存在理想 I 使 $M \subsetneq I \subsetneq R$. 因此 M 是极大理想. (若 R 非交换, 则 M 是极大左理想; 本课程中环均含幺交换, 故为极大理想.)
(b) 设 $\varphi : S \to S'$ 是单模同态. $\ker\varphi$ 是 S 的子模, 由 S 的单性, $\ker\varphi = 0$ 或 $\ker\varphi = S$. 若 $\ker\varphi = S$, 则 φ 是零同态.
若 $\ker\varphi = 0$, 则 φ 是单射. 因 $S \neq 0$, 像 $\operatorname{Im}\varphi$ 非零; 而 $\operatorname{Im}\varphi$ 是 S' 的子模, S' 是单模, 故 $\operatorname{Im}\varphi = S'$, φ 是满射. 于是 φ 是双射模同态, 即同构.
故 φ 要么是零同态, 要么是同构, Schur 引理得证.

习题 2.1

Let $R = \mathbb{C}[x, y]$, and let M be the ideal of R generated by the two elements x and y. Is M a free R-module?

解答

题目翻译: 设 $R = \mathbb{C}[x, y]$, M 是由 x 与 y 两个元素生成的理想. M 是自由 R-模吗?
解答:$M = (x, y)$ 不是自由 R-模.
先指出: 分式域 $K = \mathbb{C}(x, y)$ 中任意两个元素在 R 上线性相关. 设 $\alpha = a/b$, $\beta = c/d$, 其中 $a, b, c, d \in R$, $b, d \neq 0$ (若 $\alpha = 0$ 或 $\beta = 0$ 则显然相关). 则

$$(cb)\,\alpha - (ad)\,\beta = cb \cdot \frac{a}{b} - ad \cdot \frac{c}{d} = ac - ac = 0,$$

且系数 $cb, ad \in R$ 均非零.
反设 M 是自由模. 因 $M \subseteq R \subseteq K$, 若 M 的基含两个不同元素 α, β, 则它们应 R-线性无关, 与上式矛盾. 故基至多含一个元素. 又 $M \neq 0$, 基非空, 故基恰含一个元素, M

是秩 1 的自由模, 从而 $M \cong R$, 特别地 M 是主理想: $M = (f)$ 对某 $f \in R$.
但 $x, y \in (f)$ 蕴含 $f \mid x$ 且 $f \mid y$. 在唯一分解整环 $\mathbb{C}[x, y]$ 中 x, y 互素, 故 f 是单位, $(f) = R$. 这与 $M = (x, y) \neq R$ 矛盾 (例如常数 $1 \notin (x, y)$).
所以 M 不是自由 R-模.

习题 2.3

Let A be the matrix of a homomorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ of free $\mathbb{Z}$-modules.
(a) Prove that φ is injective if and only if the rank of A, as a real matrix, is n.
(b) Prove that φ is surjective if and only if the greatest common divisor of the determinants of the $m \times m$ minors of A is 1.

解答

题目翻译: 设 A 是自由 $\mathbb{Z}$-模之间的同态 $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ 的矩阵.
(a) 证明: φ 是单射当且仅当 A 作为实矩阵的秩等于 n.
(b) 证明: φ 是满射当且仅当 A 的所有 $m \times m$ 子式的行列式的最大公因数等于 1.
解答:A 是 $m \times n$ 整数矩阵, φ 把列向量 $X \in \mathbb{Z}^n$ 送到 $AX \in \mathbb{Z}^m$.
(a) 把 A 同时看成 $\mathbb{Q}$-线性映射 $\mathbb{Q}^n \to \mathbb{Q}^m$ 与实线性映射 $\mathbb{R}^n \to \mathbb{R}^m$. 矩阵的秩等于最高阶非零子式的阶数; A 的元素是整数, 子式行列式是整数, 在 $\mathbb{Q}$ 与 $\mathbb{R}$ 中 "非零" 是一致的, 故有理秩等于实秩.
若实秩等于 n, 则 $A : \mathbb{Q}^n \to \mathbb{Q}^m$ 的核为零 (秩-零化度定理), 限制到 $\mathbb{Z}^n$ 上仍为单射, 即 φ 单.
反之, 设 φ 单. 若实秩 $< n$, 则 $A : \mathbb{Q}^n \to \mathbb{Q}^m$ 有非零核, 取非零 $X \in \mathbb{Q}^n$ 使 $AX = 0$. 选正整数 d 使 $Y = dX \in \mathbb{Z}^n$ 非零, 则 $AY = d\,AX = 0$, 与 φ 单矛盾. 故实秩为 n.
因此 φ 单当且仅当 $\operatorname{rank} A = n$.
(b) 记 $L = \operatorname{Im} \varphi$, 即 A 的列向量在 $\mathbb{Z}^m$ 中生成的子模. Smith 标准形定理说: 主理想整环上的每个矩阵都可用可逆整初等行, 列变换化为对角形, 且对角元 $d_1 \mid d_2 \mid \cdots$. 于是存在 $P \in \mathrm{GL}_m(\mathbb{Z})$, $Q \in \mathrm{GL}_n(\mathbb{Z})$ 使

$$PAQ = D = \operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0),$$

其中 $r = \operatorname{rank} A$, $d_i \geq 1$, $d_1 \mid d_2 \mid \cdots \mid d_r$. 换基不改变商模的同构类,

$$\mathbb{Z}^m / L \cong \mathbb{Z}^m / \operatorname{Im} D \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_r \oplus \mathbb{Z}^{m-r}.$$

故 $L = \mathbb{Z}^m$ (即 φ 满) 当且仅当 $r = m$ 且 $d_1 = \cdots = d_m = 1$, 当且仅当 $d_1 d_2 \cdots d_m = 1$.
另一方面, 乘以可逆整数矩阵不改变全体 $m \times m$ 子式行列式的最大公因数: 由 Cauchy-Binet 公式, PAQ 的每个 $m \times m$ 子式是 A 的 $m \times m$ 子式的整数线性组合, 反之亦然. 对 D 而言, $m \times m$ 子式是 m 个非零对角元的乘积; 若 $r < m$, 则所有 $m \times m$ 子式都是 0, 最大公因数为 0; 若 $r \geq m$, 则最大公因数为 $d_1 d_2 \cdots d_m$ (因为 $d_1 \mid \cdots \mid d_r$ 使

$d_1 \cdots d_m$ 整除每个这样的乘积, 且其本身是一个子式). 故 A 的 $m \times m$ 子式行列式的最大公因数恰为 $d_1 \cdots d_m$, 从而 φ 满当且仅当该最大公因数为 1.

习题 4.3

Determine all integer solutions to the system of equations $AX = 0$, when $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix}$. Find a basis for the space of integer column vectors B such that $AX = B$ has a solution.

解答

题目翻译: 设 $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix}$. 求方程组 $AX = 0$ 的所有整数解, 并求使 $AX = B$ 有解的整数列向量 B 所成空间的一组基.

解答: 设 $X = (x, y, z)^{\mathrm{T}} \in \mathbb{Z}^3$. 方程组为

$$4x + 7y + 2z = 0, \qquad 2x + 4y + 6z = 0.$$

第二个方程除以 2 得 $x + 2y + 3z = 0$, 即 $x = -2y - 3z$. 代入第一个方程:

$$4(-2y - 3z) + 7y + 2z = -y - 10z = 0,$$

故 $y = -10z$, 从而 $x = -2(-10z) - 3z = 17z$. 于是

$$(x, y, z)^{\mathrm{T}} = (17z, -10z, z)^{\mathrm{T}} = z\,(17, -10, 1)^{\mathrm{T}}, \qquad z \in \mathbb{Z}.$$

所有整数解构成秩 1 的自由 Abel 群 $\mathbb{Z} \cdot (17, -10, 1)^{\mathrm{T}}$, 一组基为 $\{(17, -10, 1)^{\mathrm{T}}\}$.

使 $AX = B$ 有解的 $B \in \mathbb{Z}^2$ 全体恰为 A 的三个列向量生成的子模 $L = \langle (4,2)^{\mathrm{T}}, (7,4)^{\mathrm{T}}, (2,6)^{\mathrm{T}} \rangle \subseteq \mathbb{Z}^2$. 由于 $\det \begin{pmatrix} 4 & 7 \\ 2 & 4 \end{pmatrix} = 2 \neq 0$, L 是 $\mathbb{Z}^2$ 中有限指数的子格.

L 中每个向量的第二个分量 $2a + 4b + 6c = 2(a + 2b + 3c)$ 都是偶数, 故 $L \subseteq \{(b_1, b_2)^{\mathrm{T}} : b_2 \text{ 为偶数}\}$. 反向包含也成立: 解

$$4a + 7b + 2c = 1, \quad 2a + 4b + 6c = 0$$

得 $a = 2, b = -1, c = 0$, 故 $(1, 0)^{\mathrm{T}} \in L$; 解

$$4a + 7b + 2c = 0, \quad 2a + 4b + 6c = 2$$

得 $a=-7, b=4, c=0$, 故 $(0,2)^{\mathrm{T}} \in L$. 所以

$$L=\{(b_1,b_2)^{\mathrm{T}} \in \mathbb{Z}^2 : b_2 \equiv 0 \pmod 2\},$$

其一组基为 $\{(1,0)^{\mathrm{T}}, (0,2)^{\mathrm{T}}\}$.
核对: A 的三个 2×2 子式行列式为 $2, 20, 34$, 最大公因数为 2, 恰为指数 $[\mathbb{Z}^2 : L]$.

习题 7.1

Find a direct sum of cyclic groups isomorphic to the abelian group presented by the matrix $\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$.

解答

题目翻译: 求与矩阵 $\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$ 给出的 Abel 群同构的循环群直和.

解答: 记 $A=\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$. 该矩阵给出的 Abel 群是 $G=\mathbb{Z}^3/\operatorname{Im} A$, 其中 $\operatorname{Im} A$ 由 A 的三列生成.
求 A 的 Smith 标准形, 依次做整初等行列变换:

$$A=\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix} \xrightarrow{R_1\leftarrow R_1-R_2} \begin{pmatrix} 0 & 0 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix} \xrightarrow{R_2\leftarrow R_2-R_3} \begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & -2 \\ 2 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{R_1\leftrightarrow R_3} \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{C_3\leftarrow C_3-C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{C_3\leftarrow C_3+C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

故 A 的 Smith 标准形为 $\operatorname{diag}(2,2,2)$, 不变因子为 $d_1=d_2=d_3=2$.
有限生成 Abel 群基本定理说: 每个有限生成 Abel 群同构于循环群的直和, 且由矩阵的不变因子决定. 因此

$$G \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 = (\mathbb{Z}/2)^3.$$

核对: $|\det A| = 8 = |(\mathbb{Z}/2)^3|$.

习题 7.2

Write the abelian group generated by x and y, with the relation $3x+4y=0$ as a direct sum of cyclic groups.

解答

题目翻译: 把由 x, y 生成, 满足关系 $3x+4y=0$ 的 Abel 群写成循环群的直和.
解答: 该群是 $G = \mathbb{Z}^2/\langle(3,4)^{\mathrm{T}}\rangle$, 其中 $\langle(3,4)^{\mathrm{T}}\rangle$ 是关系向量生成的子群. 由于 $\gcd(3,4)=1$, 向量 $(3,4)^{\mathrm{T}}$ 是 $\mathbb{Z}^2$ 中的本原向量, 可扩展为一组基. 具体地, 令

$$u = x + y, \qquad v = 3x + 4y.$$

从 (u,v) 到 (x,y) 的过渡矩阵为 $\begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}$, 行列式等于 $4-3=1$, 故 $\{u,v\}$ 是自由 Abel 群 $\mathbb{Z}x \oplus \mathbb{Z}y$ 的一组基. 关系 $v=0$ 说明在商群中消去基向量 v, 故

$$G \cong \mathbb{Z}u \cong \mathbb{Z},$$

即 G 同构于无穷循环群 $\mathbb{Z}$ (作为循环群的直和只有一个直和项). 在 G 中 $u = x+y$ 是生成元, 且有 $x = 4u$, $y = -3u$.

习题 8.1

Let T be the linear operator on $\mathbb{C}^2$ whose matrix is $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. Is the corresponding $\mathbb{C}[t]$-module cyclic?

解答

题目翻译: 设 T 是 $\mathbb{C}^2$ 上的线性算子, 其矩阵为 $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. 相应的 $\mathbb{C}[t]$-模是循环模吗?
解答: 在相应的 $\mathbb{C}[t]$-模结构中, t 的作用由 T 给出: $t \cdot v = Tv$.
取 $v = (1,1)^{\mathrm{T}}$. 则

$$t \cdot v = Tv = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

v 与 tv 张成整个 $\mathbb{C}^2$, 因为

$$\det \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix} = 1 - 3 = -2 \neq 0.$$

由 v 生成的子模 $\mathbb{C}[t] \cdot v$ 含有 v 与 $t \cdot v$, 故含有它们的一切 $\mathbb{C}$-线性组合, 即整个 $\mathbb{C}^2$. 因此 $\mathbb{C}[t] \cdot v = \mathbb{C}^2$, 该模是循环模, 且 $v = (1, 1)^{\mathrm{T}}$ 是一个生成元.
判据补充: T 的特征多项式为 $(t-1)(t-2)$, 两个特征值互异, 故最小多项式等于特征多项式, 其次数等于 $\dim_{\mathbb{C}} \mathbb{C}^2 = 2$, 这等价于存在循环向量. 这里 v 不属于任何特征子空间 (特征值 2 对应特征向量 $(1, 0)^{\mathrm{T}}$, 特征值 1 对应 $(1, -1)^{\mathrm{T}}$), 故确为循环向量.

习题 2.2

Prove that a ring R having the property that every finitely generated R-module is free is either a field or the zero ring.

解答

题目翻译: 证明: 若环 R 的每个有限生成 R-模都是自由模, 则 R 要么是域, 要么是零环.
解答: 按本课程约定, 环均指含单位元的交换环. 若 $R = 0$, 则唯一的模是零模 0, 它是自由模, 结论成立. 下设 $R \neq 0$, 证明 R 是域.
先说明一个事实: 非零交换环上的循环自由模只能是 R 或 0. 设循环模 $M \cong R^n$. 取 R 的极大理想 $\mathfrak{m}$, 则 $M/\mathfrak{m}M \cong (R/\mathfrak{m})^n$ 是域 $R/\mathfrak{m}$ 上的 n 维线性空间. 因 M 循环, $M/\mathfrak{m}M$ 由一个元素生成, 故 $n \leq 1$. 所以 $M \cong R$ 或 $M = 0$.
对任意理想 I, 商模 R/I 由 $1 + I$ 生成, 是循环模, 故有限生成, 由假设是自由模, 于是 $R/I \cong R$ 或 $R/I = 0$.

- 若 $R/I = 0$, 则 $I = R$.
- 若 $R/I \cong R$, 则自然满射 $R \to R/I$ 复合同构 $R/I \cong R$ 得 R 的一个满自同态 f. 设 $a = f(1)$, 则 $f(r) = ra$; 满射给出 $aR = R$, 故 a 是单位, f 是同构, 其核为 0, 即 $I = 0$.

于是 R 的理想只有 0 与 R 两个. 对任意非零 $a \in R$, 主理想 $(a) \neq 0$, 故 $(a) = R$, 存在 $b \in R$ 使 $ab = 1$, 即 a 是单位. 因此 R 是域.

习题 2.4

Let I be an ideal of a ring R.
(a) Under what circumstances is I a free R-module?
(b) Under what circumstances is the quotient ring R/I a free R-module?

解答

题目翻译: 设 I 是环 R 的一个理想.
(a) 在什么情况下 I 是自由 R-模?
(b) 在什么情况下商环 R/I 是自由 R-模?
解答: 环均指含单位元的交换环.
(a) I 是自由 R-模当且仅当 $I=0$, 或 $I=(a)$ 且 a 是非零因子 (即 $\mathrm{Ann}(a)=\{r\in R\mid ra=0\}=0$). 特别地, 当 R 是整环时, 这等价于 $I=0$ 或 I 是非零主理想.
先证充分性. 若 $I=(a)$ 且 $\mathrm{Ann}(a)=0$, 则映射 $R\to I$, $r\mapsto ra$ 是 R-模同构: 满射由 $(a)=Ra$ 的定义, 单射因 $\mathrm{Ann}(a)=0$. 故 $I\cong R$ 是自由模.
再证必要性. 设 $I\neq 0$ 是自由模, 取一组基 $\{e_\lambda\}$. 基中元素均非零, 否则 $1\cdot 0=0$ 是非平凡线性关系. 又因环交换且 $I\subseteq R$, 对基中任意两个元素 e_λ, e_μ 有

$$e_\mu e_\lambda - e_\lambda e_\mu = 0,$$

这是系数分别为 e_μ 与 $-e_\lambda$ 的线性关系. 若基含有两个不同元素, 线性无关性迫使 $e_\mu=0$ 且 $e_\lambda=0$, 矛盾. 故基恰含一个元素, 设其为 a, 则 $I=(a)$. 又非零循环自由模同构于 R, 故 $Ra\cong R$; 而同构 $R\to Ra$, $r\mapsto ra$ 的核是 $\mathrm{Ann}(a)$, 故 $\mathrm{Ann}(a)=0$, 即 a 是非零因子.
(b) R/I 是自由 R-模当且仅当 $I=0$ 或 $I=R$.
R/I 由 $1+I$ 生成, 是循环模. 若 R/I 是自由模, 则 $R/I\cong R^n$; 循环模迫使 $n\leq 1$ (论证同习题 2.2 中的事实: 取极大理想 $\mathfrak{m}$, 商去 $\mathfrak{m}$ 得域上由单元素生成的 n 维空间), 故 $R/I\cong R$ 或 $R/I=0$. 若 $R/I=0$ 则 $I=R$; 若 $R/I\cong R$, 则自然满射 $R\to R/I\cong R$ 是 R 的满自同态, 它是乘以单位映射, 从而是同构, 核为 0, 即 $I=0$. 反之, $I=0$ 时 $R/I=R$ 是自由模, $I=R$ 时 $R/I=0$ 也是自由模.

习题 7.5

Determine the number of isomorphism classes of abelian groups of order 400.

解答

题目翻译: 求 400 阶 Abel 群的同构类的个数.
解答: 分解 $400=2^4\times 5^2$. 有限生成 Abel 群基本定理说: 每个有限 Abel 群同构于循环群的直和, 且同构类由其 p-部分独立决定. 于是 400 阶 Abel 群 G 唯一地写成

$$G\cong P_2\oplus P_5,$$

其中 P_2 是阶为 $2^4=16$ 的 2-群, P_5 是阶为 $5^2=25$ 的 5-群.
P_2 的同构类由 4 的整数分拆给出, 共有 5 种:

$$4,\quad 3+1,\quad 2+2,\quad 2+1+1,\quad 1+1+1+1,$$

分别对应 $\mathbb{Z}/16$, $\mathbb{Z}/8\oplus\mathbb{Z}/2$, $\mathbb{Z}/4\oplus\mathbb{Z}/4$, $\mathbb{Z}/4\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2$, $(\mathbb{Z}/2)^4$.
P_5 的同构类由 2 的整数分拆给出, 共有 2 种:

$$2, \qquad 1+1,$$

分别对应 $\mathbb{Z}/25$ 与 $\mathbb{Z}/5\oplus\mathbb{Z}/5$.
两部分独立搭配, 故同构类总数为

$$5\times 2 = 10.$$

4

第四次作业

习题 1.1

Let R be an integral domain that contains a field F as subring and that is finite-dimensional when viewed as vector space over F. Prove that R is a field.

解答

题目翻译: 设 R 是一个整环, 它包含一个域 F 作为子环, 并且 R 作为 F 上的向量空间是有限维的. 证明 R 是一个域.
解答: 由于 $F\subseteq R$ 且 F 是域, R 通过数乘 $c\cdot r$ ($c\in F$, $r\in R$) 构成一个 F-向量空间, 按题意其维数有限. 任取非零元 $a\in R$, 定义 F-线性映射

$$m_a : R\to R, \quad x\mapsto ax.$$

若 $ax=0$, 则因 R 是整环且 $a\neq 0$, 得 $x=0$, 故 m_a 是单射. 有限维向量空间上的单线性映射必为满射, 故 m_a 是双射, 存在 $b\in R$ 使得 $m_a(b)=1$, 即 $ab=1$. 所以 a 在 R 中可逆. a 是任意非零元, 故 R 的每个非零元都可逆, R 是域.

习题 2.1

Let α be a complex root of the polynomial x^3-3x+4. Find the inverse of $\alpha^2+\alpha+1$ in the form $a+b\alpha+c\alpha^2$, with a,b,c in $\mathbb{Q}$.

解答

题目翻译: 设 α 是多项式 x^3-3x+4 的一个复根. 求 $\alpha^2+\alpha+1$ 的逆元, 写成 $a+b\alpha+c\alpha^2$ 的形式, 其中 $a,b,c\in\mathbb{Q}$.

解答: 先验证 $f(x)=x^3-3x+4$ 在 $\mathbb{Q}$ 上不可约. 有理根必为 $\pm1,\pm2,\pm4$, 直接代入均不为 0, 三次多项式无有理根故不可约, 因此 $\mathbb{Q}(\alpha)$ 是域且 $\{1,\alpha,\alpha^2\}$ 是它在 $\mathbb{Q}$ 上的一组基. 由 $f(\alpha)=0$ 得

$$\alpha^3=3\alpha-4,\qquad \alpha^4=\alpha(3\alpha-4)=3\alpha^2-4\alpha.$$

设 $(\alpha^2+\alpha+1)(a+b\alpha+c\alpha^2)=1$. 展开左端并利用上面两式把 α^3,α^4 约化, 得

$$(\alpha^2+\alpha+1)(a+b\alpha+c\alpha^2)=(a-4b-4c)+(a+4b-c)\alpha+(a+b+4c)\alpha^2.$$

比较基 $\{1,\alpha,\alpha^2\}$ 的系数, 得线性方程组

$$a-4b-4c=1,\qquad a+4b-c=0,\qquad a+b+4c=0.$$

解之得 $a=\frac{17}{49}$, $b=-\frac{5}{49}$, $c=-\frac{3}{49}$. 于是

$$(\alpha^2+\alpha+1)^{-1}=\frac{17}{49}-\frac{5}{49}\alpha-\frac{3}{49}\alpha^2.$$

习题 2.3

Let $\beta=\omega\sqrt[3]{2}$, where $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$, and let $K=\mathbb{Q}(\beta)$. Prove that the equation $x_1^2+\cdots+x_k^2=-1$ has no solution with x_i in K.

解答

题目翻译: 设 $\beta=\omega\sqrt[3]{2}$, 其中 $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$, 令 $K=\mathbb{Q}(\beta)$. 证明方程 $x_1^2+\cdots+x_k^2=-1$ 在 K 中没有解 (即不存在 $x_i\in K$ 满足该式).

解答: 因为 $\omega^3=1$, 所以 $\beta^3=2$, 即 β 是 x^3-2 的根. x^3-2 在 $\mathbb{Q}$ 上由 Eisenstein 判据 (取 $p=2$) 不可约, 于是 $[K:\mathbb{Q}]=3$ 且 $K\cong\mathbb{Q}[x]/(x^3-2)$. 把 x 送到 $\sqrt[3]{2}$ 得到 $\mathbb{Q}$ 嵌入 $\varphi:K\to\mathbb{R}$, 满足 $\varphi(\beta)=\sqrt[3]{2}$, 其像 $\varphi(K)=\mathbb{Q}(\sqrt[3]{2})$ 是实数域的子域.

假设方程在 K 中有解, 即存在 $x_1,\dots,x_k\in K$ 使 $x_1^2+\cdots+x_k^2=-1$. 对两边作用 φ, 得

$$\varphi(x_1)^2+\cdots+\varphi(x_k)^2=-1.$$

但每个 $\varphi(x_i)\in\mathbb{R}$, 实数的平方非负, 左端是 k 个非负实数之和, 应当大于等于 0, 而右端为 $-1<0$, 矛盾. 故该方程在 K 中无解.

习题 3.2

Prove that the polynomial x^4+3x+3 is irreducible over the field $\mathbb{Q}[\sqrt[3]{2}]$.

解答

题目翻译: 证明多项式 x^4+3x+3 在域 $\mathbb{Q}[\sqrt[3]{2}]$ 上不可约.

解答: 记 $f(x)=x^4+3x+3$, $K=\mathbb{Q}(\sqrt[3]{2})$. 由 Eisenstein 判据 (取 $p=3$), $3\mid 3$, $3\mid 3$, 但 $9\nmid 3$, 故 f 在 $\mathbb{Q}$ 上不可约; x^3-2 也由 Eisenstein 判据 (取 $p=2$) 在 $\mathbb{Q}$ 上不可约, 故 $[K:\mathbb{Q}]=3$.

反设 f 在 K 上可约. f 是四次多项式, 于是 f 在 K 上必有一次或二次不可约因子, 取其中一个不可约因子 g, 设 α 是 g 的一个根, 则 α 也是 f 的根, 且 $d:=\deg g\in\{1,2\}$. 于是

$$[K(\alpha):K]=d,\qquad [K(\alpha):\mathbb{Q}]=[K(\alpha):K]\,[K:\mathbb{Q}]=3d\in\{3,6\}.$$

另一方面, 因 f 在 $\mathbb{Q}$ 上不可约且 α 是 f 的根, f 就是 α 在 $\mathbb{Q}$ 上的极小多项式, 故 $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. 而 $\mathbb{Q}(\alpha)\subseteq K(\alpha)$, 由次数公式 $[\mathbb{Q}(\alpha):\mathbb{Q}]$ 整除 $[K(\alpha):\mathbb{Q}]=3d$, 即 $4\mid 3d$. 但 $d\in\{1,2\}$ 时 $3d\in\{3,6\}$ 均不被 4 整除, 矛盾. 故 f 在 K 上不可约.

习题 3.6

Let a be a positive rational number that is not a square in $\mathbb{Q}$. Prove that $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$.

解答

题目翻译: 设 a 是正有理数且不是 $\mathbb{Q}$ 中的平方数. 证明 $\sqrt[4]{a}$ 在 $\mathbb{Q}$ 上的次数为 4.

解答: 记 $\alpha=\sqrt[4]{a}$. 因为 a 是正数且非平方, 多项式 x^2-a 在 $\mathbb{Q}$ 上无根, 故不可约, $[\mathbb{Q}(\sqrt{a}):\mathbb{Q}]=2$.

先证 $\alpha\notin\mathbb{Q}(\sqrt{a})$. 反设 $\alpha=p+q\sqrt{a}$ $(p,q\in\mathbb{Q})$, 则

$$\alpha^2=p^2+aq^2+2pq\sqrt{a}=\sqrt{a},$$

比较 $\{1,\sqrt{a}\}$ 的系数得 $p^2+aq^2=0$ 且 $2pq=1$. 由 $2pq=1$ 知 $p,q\neq 0$, 于是 $a=-(p/q)^2<0$, 与 $a>0$ 矛盾. 故 $\alpha\notin\mathbb{Q}(\sqrt{a})$, 多项式 $x^2-\sqrt{a}$ 在 $\mathbb{Q}(\sqrt{a})$ 上无根 (次数为 2, 无根即不可约), 从而 $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{a})]=2$.

用次数公式 $[K:F]=[K:L][L:F]$ 得

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{a})]\,[\mathbb{Q}(\sqrt{a}):\mathbb{Q}]=2\cdot 2=4.$$

即 $\sqrt[4]{a}$ 在 $\mathbb{Q}$ 上的次数为 4.

习题 3.7

(a) Is i in the field $\mathbb{Q}(\sqrt[4]{-2})$? (b) Is $\sqrt[3]{5}$ in the field $\mathbb{Q}(\sqrt[3]{2})$?

解答

题目翻译:(a) i 是否属于域 $\mathbb{Q}(\sqrt[4]{-2})$? (b) $\sqrt[3]{5}$ 是否属于域 $\mathbb{Q}(\sqrt[3]{2})$?

解答:(a) 答案是否定的. 记 $\alpha=\sqrt[4]{-2}$, 则 $\alpha^4=-2$, 即 α 是 x^4+2 的根. x^4+2 在 $\mathbb{Q}$ 上由 Eisenstein 判据 (取 $p=2$) 不可约, 故 $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. 又 $\alpha\cdot\sqrt[4]{2}=\sqrt[4]{-4}=1+i$ (因为 $(-4)^{1/4}=\sqrt{2}\,\mathrm{e}^{\pi i/4}=1+i$), 所以 $\sqrt[4]{2}=(1+i)/\alpha$. 若 $i\in\mathbb{Q}(\alpha)$, 则 $1+i\in\mathbb{Q}(\alpha)$, 从而 $\sqrt[4]{2}=(1+i)/\alpha\in\mathbb{Q}(\alpha)$, 于是 $\mathbb{Q}(\sqrt[4]{2},i)\subseteq\mathbb{Q}(\alpha)$. 但 $[\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}]=8$: 因为 $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$ (x^4-2 由 Eisenstein 判据不可约), 而 $\mathbb{Q}(\sqrt[4]{2})\subseteq\mathbb{R}$, 故 $i\notin\mathbb{Q}(\sqrt[4]{2})$, 再添加 i 使次数翻倍. 于是 8 整除 $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$, 矛盾. 所以 $i\notin\mathbb{Q}(\sqrt[4]{-2})$.
(b) 答案也是否定的. 反设 $\sqrt[3]{5}\in\mathbb{Q}(\sqrt[3]{2})$, 把它写成

$$\sqrt[3]{5}=a+b\sqrt[3]{2}+c\sqrt[3]{4},\qquad a,b,c\in\mathbb{Q}.$$

对两边取从 $F=\mathbb{Q}(\sqrt[3]{2})$ 到 $\mathbb{Q}$ 的迹 $\mathrm{Tr}_{F/\mathbb{Q}}$. 因为 $\sqrt[3]{5}$, $\sqrt[3]{2}$, $\sqrt[3]{4}$ 的极小多项式分别是 x^3-5, x^3-2, x^3-4, 其 x^2 项系数均为 0, 故三者的迹都等于 0 (迹等于其共轭之和, 即对应多项式的三个根之和). 于是 $0=\mathrm{Tr}(\sqrt[3]{5})=3a$, 得 $a=0$. 所以

$$\sqrt[3]{5}=b\sqrt[3]{2}+c\sqrt[3]{4}=\sqrt[3]{2}\,(b+c\sqrt[3]{2}).$$

两边立方:

$$5=2(b+c\sqrt[3]{2})^3=(2b^3+4c^3)+6b^2c\,\sqrt[3]{2}+6bc^2\,\sqrt[3]{4},$$

其中用了 $(\sqrt[3]{2})^3=2$. 比较 $\mathbb{Q}$ 基 $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ 的系数, 得

$$6b^2c=0,\qquad 6bc^2=0,\qquad 2b^3+4c^3=5.$$

前两式推出 $b=0$ 或 $c=0$. 若 $b=0$, 则 $4c^3=5$, $c^3=5/4$, 与 $c\in\mathbb{Q}$ 矛盾; 若 $c=0$, 则 $2b^3=5$, $b^3=5/2$, 同样矛盾. 因此 $\sqrt[3]{5}\notin\mathbb{Q}(\sqrt[3]{2})$.

习题 3.9

Let α and β be complex roots of irreducible polynomials $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$. Let $K=\mathbb{Q}(\alpha)$ and $L=\mathbb{Q}(\beta)$. Prove that $f(x)$ is irreducible in $L[x]$ if and only if $g(x)$ is irreducible in $K[x]$.

解答

题目翻译: 设 α 与 β 分别是 $\mathbb{Q}[x]$ 中不可约多项式 $f(x)$ 与 $g(x)$ 的复根. 令 $K=\mathbb{Q}(\alpha)$, $L=\mathbb{Q}(\beta)$. 证明 $f(x)$ 在 $L[x]$ 中不可约当且仅当 $g(x)$ 在 $K[x]$ 中不可约.

解答: 不妨设 f, g 首一 (乘以非零常数不改变不可约性). 因为 f 在 $\mathbb{Q}$ 上不可约且 α 是 f 的根, f 是 α 的极小多项式, 故 $m := [K : \mathbb{Q}] = \deg f$; 同理 $n := [L : \mathbb{Q}] = \deg g$.
f 在 $L[x]$ 中不可约 $\Longleftrightarrow$ α 在 L 上的极小多项式仍是 f (次数为 m) $\Longleftrightarrow$ $[L(\alpha) : L] = m$ $\Longleftrightarrow$

$$[L(\alpha) : \mathbb{Q}] = [L(\alpha) : L]\,[L : \mathbb{Q}] = mn.$$

类似地, g 在 $K[x]$ 中不可约 $\Longleftrightarrow$ $[K(\beta) : K] = n$ $\Longleftrightarrow$ $[K(\beta) : \mathbb{Q}] = nm$.
但 $L(\alpha) = \mathbb{Q}(\beta)(\alpha) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)(\beta) = K(\beta)$, 所以 $[L(\alpha) : \mathbb{Q}] = [K(\beta) : \mathbb{Q}]$. 两个条件等价于同一个整数 mn, 故二者等价.

习题 3.10

A field extension K/F is an algebraic extension if every element of K is algebraic over F. Let K/F and L/K be algebraic field extensions. Prove that L/F is an algebraic extension.

解答

题目翻译: 域扩张 K/F 称为代数扩张, 若 K 中每个元素都在 F 上代数. 设 K/F 与 L/K 都是代数扩张. 证明 L/F 是代数扩张.
解答: 任取 $\gamma \in L$. 因 L/K 是代数扩张, γ 在 K 上代数, 故存在非零多项式 $c_0 + c_1 x + \cdots + c_n x^n \in K[x]$ 以 γ 为根. 记 $K' = F(c_0, c_1, \ldots, c_n) \subseteq K$. 由于 K/F 是代数扩张, 每个 c_i 都在 F 上代数, 依次添加 $c_0, \ldots, c_n$ 得到的 K' 在 F 上的次数是有限的 (每次添加代数元得到的单扩张次数有限, 再用次数公式 $[K' : F] = [K' : F(c_0, \ldots, c_{n-1})] \cdots [F(c_0) : F]$). 又 γ 满足同一个多项式, 故 γ 在 K' 上代数, $[K'(\gamma) : K']$ 有限. 于是

$$[K'(\gamma) : F] = [K'(\gamma) : K']\,[K' : F]$$

有限, 所以 γ 在 F 上代数 (有限扩张是代数扩张). γ 是 L 中任意元素, 故 L/F 是代数扩张.

习题 4.3

With reference to Example 15.4.4(b), determine the irreducible polynomial for $\gamma = \alpha_1 + \alpha_2$ over $\mathbb{Q}$.

解答

题目翻译: 参照 Example 15.4.4(b), 求 $\gamma = \alpha_1 + \alpha_2$ 在 $\mathbb{Q}$ 上的不可约多项式.
解答: 按 Example 15.4.4(b) 的设定, $\alpha_1 = \sqrt[3]{2}$ 与 $\alpha_2 = \omega\sqrt[3]{2}$ 是 $x^3 - 2$ 的两个根, 其中 $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$. 令 $\gamma = \alpha_1 + \alpha_2 = \sqrt[3]{2}(1 + \omega)$. 由 $1 + \omega = \mathrm{e}^{\pi\mathrm{i}/3}$, 得

$$\gamma^3 = (\sqrt[3]{2})^3\,(1 + \omega)^3 = 2 \cdot (\mathrm{e}^{\pi\mathrm{i}/3})^3 = 2\,\mathrm{e}^{\pi\mathrm{i}} = -2.$$

故 γ 是 x^3+2 的根. x^3+2 在 $\mathbb{Q}$ 上由 Eisenstein 判据 (取 $p=2$) 不可约, 它是首一的, 所以 x^3+2 正是 γ 在 $\mathbb{Q}$ 上的不可约多项式.

习题 7.2

Determine the irreducible polynomial of each of the elements of $\mathbb{F}_8$ in the list 15.7.8.

解答

题目翻译: 求 15.7.8 的列表中 $\mathbb{F}_8$ 的每个元素在 $\mathbb{F}_2$ 上的不可约多项式 (即极小多项式).

解答: 设 α 是 $f(x)=x^3+x+1$ 在 $\mathbb{F}_2$ 上的一个根, 则 $\mathbb{F}_8=\mathbb{F}_2(\alpha)$, 且由 $\alpha^3+\alpha+1=0$ (在 $\mathbb{F}_2$ 中 $-1=1$) 得 $\alpha^3=\alpha+1$. 列表中的 8 个元素用 α 表示:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1,\ \alpha^2+1.$$

其幂次对应为 $\alpha^3=\alpha+1$, $\alpha^4=\alpha^2+\alpha$, $\alpha^5=\alpha^2+\alpha+1$, $\alpha^6=\alpha^2+1$, $\alpha^7=1$. Frobenius 映射 $t\mapsto t^2$ 在 $\mathbb{F}_8/\mathbb{F}_2$ 上给出共轭作用, 同共轭类中的元素共用一个极小多项式. 逐类计算得:

0 的极小多项式为 x;

1 的极小多项式为 $x+1$;

$\alpha, \alpha^2, \alpha^4=\alpha^2+\alpha$ 的极小多项式为 x^3+x+1 (其中 α 是定义根, α^2 与 α^4 是它在 Frobenius 映射下的共轭);

$\alpha^3=\alpha+1$, $\alpha^5=\alpha^2+\alpha+1$, $\alpha^6=\alpha^2+1$ 的极小多项式为 x^3+x^2+1.

验证后一类: 记 $g(x)=x^3+x^2+1$, 逐一代入 $g(\alpha+1)$, $g(\alpha^5)$, $g(\alpha^6)$ 均得 0; 例如 $g(\alpha+1)=(\alpha+1)^3+(\alpha+1)^2+1$, 其中 $(\alpha+1)^2=\alpha^2+1$, $(\alpha+1)^3=\alpha^3+\alpha^2+\alpha+1=\alpha^2$, 故 $g(\alpha+1)=\alpha^2+(\alpha^2+1)+1=0$. $\mathbb{F}_2$ 上三次不可约多项式只有 x^3+x+1 与 x^3+x^2+1 两个, 这 6 个非零非 1 元素分成两个共轭类, 恰好各以其中一个为极小多项式.

习题 7.8

The polynomials $f(x)=x^3+x+1$ and $g(x)=x^3+x^2+1$ are irreducible over $\mathbb{F}_2$. Let K be the field extension obtained by adjoining a root of f, and let L be the extension obtained by adjoining a root of g. Describe explicitly an isomorphism from K to L, and determine the number of such isomorphisms.

解答

题目翻译: 多项式 $f(x)=x^3+x+1$ 与 $g(x)=x^3+x^2+1$ 在 $\mathbb{F}_2$ 上不可约. 设 K 是添加 f 的一个根得到的域扩张, L 是添加 g 的一个根得到的扩张. 明确描述一个从 K 到 L 的同构, 并确定这样的同构的个数.

解答: 记 $K=\mathbb{F}_2[\alpha]$, 其中 $\alpha^3+\alpha+1=0$ (故 $\alpha^3=\alpha+1$); 记 $L=\mathbb{F}_2[\beta]$, 其中

$\beta^3+\beta^2+1=0$ (故 $\beta^3=\beta^2+1$). 在 L 中找 f 的根: 因 $(\beta+1)^2=\beta^2+1$,

$$(\beta+1)^3=(\beta+1)(\beta^2+1)=\beta^3+\beta^2+\beta+1=(\beta^2+1)+\beta^2+\beta+1=\beta,$$

于是 $f(\beta+1)=(\beta+1)^3+(\beta+1)+1=\beta+\beta+1+1=0$. 所以 $\beta+1$ 是 f 在 L 中的一个根.
由 f 在 $\mathbb{F}_2$ 上不可约, $\mathbb{F}_2(\alpha)\cong\mathbb{F}_2[x]/(f(x))$; 把 α 送到 f 的根 $\beta+1\in L$, 就唯一确定一个 $\mathbb{F}_2$ 同态 $\varphi: K\to L$, 使 $\varphi(\alpha)=\beta+1$. 这是域同态从而是单射, 而 $|K|=|L|=8$, 单射必为双射, 故 φ 是域同构. 具体地, 对 $a,b,c\in\mathbb{F}_2$,

$$\varphi(a+b\alpha+c\alpha^2)=a+b(\beta+1)+c(\beta+1)^2=(a+b+c)+b\beta+c\beta^2.$$

这样的同构的个数等于 f 在 L 中根的个数. f 在 L 中的全部根为 $\{\beta+1,\beta^2+\beta,\beta^2+1\}$ (由 Frobenius 共轭: $(\beta+1)^2=\beta^2+1$, $(\beta^2+1)^2=\beta^2+\beta$), 共 3 个. 把 α 送到这 3 个根分别得到 3 个互不相同的同构, 故共有 3 个.

习题 7.5

Factor x^9-x and $x^{27}-x$ in $\mathbb{F}_3$.

解答

题目翻译: 在 $\mathbb{F}_3$ 中分解 x^9-x 与 $x^{27}-x$.
解答: 在 $\mathbb{F}_3$ 中, $x^3-x=x(x-1)(x+1)$ 恰以 $\mathbb{F}_3=\{0,1,2\}$ 的三个元素为根. $\mathbb{F}_3$ 上的二次不可约多项式共 3 个, 逐一检验无根 ($0^2,1^2,2^2$ 代入均不为 0) 可得

$$x^2+1,\qquad x^2+x+2,\qquad x^2+2x+2.$$

对 x^9-x: 其根恰为 $\mathbb{F}_9$ 的全部元素 ($\mathbb{F}_9$ 中每个元素满足 $x^9=x$), 故在 $\mathbb{F}_3$ 上的不可约因子是 $\mathbb{F}_3$ 上次数整除 $[\mathbb{F}_9:\mathbb{F}_3]=2$ 的首一不可约多项式, 即所有一次和二次不可约多项式. 直接相乘验证:

$$(x^3-x)(x^2+1)(x^2+x+2)(x^2+2x+2)=x^9-x.$$

故

$$x^9-x=x(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

对 $x^{27}-x$: 其根恰为 $\mathbb{F}_{27}$ 的全部元素, 在 $\mathbb{F}_3$ 上的不可约因子是次数整除 $[\mathbb{F}_{27}:\mathbb{F}_3]=3$ 的首一不可约多项式, 即一次的和三次的. 一次的有 3 个: x, $x-1$, $x+1$. 三次不可约

多项式的个数为 $\frac{1}{3}(3^3-3)=8$, 逐个检验无根即得全部 8 个:

$$x^3+2x+1,\quad x^3+x^2+2x+1,\quad x^3+2x^2+1,\quad x^3+2x^2+x+1,$$
$$x^3+2x+2,\quad x^3+x^2+2,\quad x^3+x^2+x+2,\quad x^3+2x^2+2x+2.$$

(三次多项式无根当且仅当不可约, 检验方法: 依次代入 $0,1,2\in\mathbb{F}_3$ 看是否为 0.) 因此

$$x^{27}-x=x(x-1)(x+1)\prod_{i=1}^{8}p_i(x),$$

其中 $p_1(x),\dots,p_8(x)$ 为上列 8 个三次多项式.

习题 7.6

Factor the polynomial $x^{16}-x$ over the fields $\mathbb{F}_4$ and $\mathbb{F}_8$.

解答

题目翻译: 在域 $\mathbb{F}_4$ 与 $\mathbb{F}_8$ 上分解多项式 $x^{16}-x$.

解答:$x^{16}-x$ 的根恰为 $\mathbb{F}_{16}$ 的全部元素, 它在基域上的不可约因子就是 $\mathbb{F}_{16}$ 各元素在基域上的极小多项式.

在 $\mathbb{F}_4$ 上: 写 $\mathbb{F}_4=\mathbb{F}_2[\alpha]$, $\alpha^2+\alpha+1=0$ (故 $\alpha^2=\alpha+1$). 因 $[\mathbb{F}_{16}:\mathbb{F}_4]=2$, 极小多项式的次数为 1 或 2. $\mathbb{F}_4$ 的 4 个元素给出 4 个一次因子, 其余 12 个元素在 Frobenius 映射 $t\mapsto t^4$ 下分成 6 个共轭类, 给出 6 个二次不可约因子. 取 $\mathbb{F}_{16}=\mathbb{F}_2[\gamma]$, $\gamma^4=\gamma+1$ (即 γ 是 x^4+x+1 的根), 此时 $\mathbb{F}_4=\{0,1,\gamma^5,\gamma^{10}\}$, 二次因子按 $(x-t)(x-t^4)$ 计算, 得

$$\begin{aligned}x^{16}-x=x(x-1)&(x-\alpha)(x-\alpha-1)\\&\cdot(x^2+x+\alpha)(x^2+x+\alpha+1)(x^2+(\alpha+1)x+1)\\&\cdot(x^2+\alpha x+1)(x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+(\alpha+1)).\end{aligned}$$

例如 γ 的极小多项式为 $(x-\gamma)(x-\gamma^4)=x^2+x+\gamma^5=x^2+x+\alpha$; 其余 5 个二次因子分别由共轭类 $\{\gamma^2,\gamma^8\}$, $\{\gamma^3,\gamma^{12}\}$, $\{\gamma^6,\gamma^9\}$, $\{\gamma^7,\gamma^{13}\}$, $\{\gamma^{11},\gamma^{14}\}$ 算出.

在 $\mathbb{F}_8$ 上: 取 $\mathbb{F}_{16}=\mathbb{F}_2[\gamma]$, $\gamma^4=\gamma+1$. 直接计算三个轨道 $\{\gamma,\gamma^2,\gamma^4,\gamma^8\}$, $\{\gamma^3,\gamma^6,\gamma^9,\gamma^{12}\}$, $\{\gamma^7,\gamma^{11},\gamma^{13},\gamma^{14}\}$ 在 Frobenius 映射 $t\mapsto t^8$ (它是固定 $\mathbb{F}_8$ 的自同构, 因 $x^8=x$ 对一切 $x\in\mathbb{F}_8$ 成立; 其在根集 $\mathbb{F}_{16}$ 上的轨道给出 $\mathbb{F}_8$ 上的共轭类) 下不变, 对应 3 个四次不可约因子:

$$\begin{aligned}(x-\gamma)(x-\gamma^2)(x-\gamma^4)(x-\gamma^8)&=x^4+x+1,\\(x-\gamma^3)(x-\gamma^6)(x-\gamma^9)(x-\gamma^{12})&=x^4+x^3+x^2+x+1,\\(x-\gamma^7)(x-\gamma^{11})(x-\gamma^{13})(x-\gamma^{14})&=x^4+x^3+1.\end{aligned}$$

例如第一式: 分组 $(x-\gamma)(x-\gamma^4)=x^2+x+\gamma^5$ 与 $(x-\gamma^2)(x-\gamma^8)=x^2+x+\gamma^{10}$, 相乘得 $(x^2+x+\gamma^5)(x^2+x+\gamma^{10})=x^4+x+1$ (用到 $\gamma^5+\gamma^{10}=1$ 与 $\gamma^{15}=1$). 再连同 $\mathbb{F}_8$ 中元素 $0,1$ 给出的一次因子 x, $x-1$ 以及 $\mathbb{F}_4$ 的极小多项式 x^2+x+1, 得

$$x^{16}-x=x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1),$$

这一分解的所有因子系数都在 $\mathbb{F}_2$ 中, 故在 $\mathbb{F}_8$ 上成立.

习题 7.13

Prove that a finite subgroup of the multiplicative group of any field F is a cyclic group.

解答

题目翻译: 证明任意域 F 的乘法群的任何有限子群都是循环群.

解答: 设 G 是 $F^\times$ 的 n 阶有限子群. 对每个 $d\mid n$, 记 a_d 为 G 中阶恰为 d 的元素的个数. 关键事实是: 若 $a_d>0$, 则 $a_d=\varphi(d)$ (Euler 函数). 事实上, 取阶为 d 的 $g\in G$, 则 g 生成的循环子群 $\langle g\rangle$ 含 d 个元素, 它们都满足 $x^d=1$; 而在域中方程 $x^d=1$ 至多有 d 个根, 故 $\{x\in F: x^d=1\}=\langle g\rangle$. d 阶循环群的生成元恰有 $\varphi(d)$ 个, 所以 $a_d=\varphi(d)$. 若 $a_d=0$, 则 $a_d\le\varphi(d)$ 平凡成立. 于是对所有 $d\mid n$ 都有 $a_d\le\varphi(d)$. 又每个元素都有某个阶 $d\mid n$, 故 $n=\sum_{d\mid n}a_d$; 而 $\sum_{d\mid n}\varphi(d)=n$. 因此

$$n=\sum_{d\mid n}a_d\le\sum_{d\mid n}\varphi(d)=n,$$

中间的不等号必须取等, 即 $a_d=\varphi(d)$ 对所有 $d\mid n$ 成立. 特别地 $a_n=\varphi(n)\ge 1$, 所以 G 有 n 阶元素, G 是 n 阶循环群.

习题 8.2

Determine all primitive elements for the extension $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ of $\mathbb{Q}$.

解答

题目翻译: 求扩张 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ 的所有本原元素.

解答:x^2-2 与 x^2-3 在 $\mathbb{Q}$ 上不可约, 且 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$ (否则 $\sqrt{3}=a+b\sqrt{2}$, 比较系数得 $a^2+2b^2=3$, $2ab=0$, 无有理数解), 故 $[K:\mathbb{Q}]=4$, $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是一组基. K 是 $(x^2-2)(x^2-3)$ 在 $\mathbb{Q}$ 上的分裂域, 故 $K/\mathbb{Q}$ 是 Galois 扩张, Galois 群同构于 $(\mathbb{Z}/2)^2$, 有三个 2 阶子群, 从而 K 恰好有三个二次中间域:

$$\mathbb{Q}(\sqrt{2}),\qquad \mathbb{Q}(\sqrt{3}),\qquad \mathbb{Q}(\sqrt{6}).$$

对 $\gamma\in K$, 其次数 $\deg\gamma$ 整除 $[K:\mathbb{Q}]=4$, 故 $\deg\gamma\in\{1,2,4\}$. 本原元素即满足

$K=\mathbb{Q}(\gamma)$ 的元素, 等价于 $\deg\gamma=4$, 等价于 γ 不属于任何真子域, 即

$$\gamma\notin\mathbb{Q}(\sqrt{2})\cup\mathbb{Q}(\sqrt{3})\cup\mathbb{Q}(\sqrt{6}).$$

把 γ 写成 $\gamma=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ $(a,b,c,d\in\mathbb{Q})$. 则 $\gamma\in\mathbb{Q}(\sqrt{2})$ 当且仅当 $c=d=0$; $\gamma\in\mathbb{Q}(\sqrt{3})$ 当且仅当 $b=d=0$; $\gamma\in\mathbb{Q}(\sqrt{6})$ 当且仅当 $b=c=0$. 因此 $K/\mathbb{Q}$ 的本原元素全体为

$$\gamma=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6},\qquad a\in\mathbb{Q},\quad b,c,d\in\mathbb{Q}\text{ 中至少两个非零.}$$

习题 3.1

Let f be a polynomial of degree n with coefficients in F and let K be a splitting field for f over F. Prove that $[K:F]$ divides $n!$.

解答

题目翻译: 设 f 是 F 上次数为 n 的多项式, K 是 f 在 F 上的一个分裂域. 证明 $[K:F]$ 整除 $n!$.
解答: 对 n 作归纳. $n=1$ 时 $K=F$, $[K:F]=1$, 成立.
设 $n\geq 2$. 若 f 可约, 写 $f=gh$, 其中 $\deg g=m$, $\deg h=n-m$, $1\leq m\leq n-1$. 取 K_1 为 K 中由 g 的根生成的子域 (它是 g 在 F 上的一个分裂域), 则 K 是 h 在 K_1 上的分裂域. 由归纳假设 $[K_1:F]\mid m!$ 且 $[K:K_1]\mid(n-m)!$, 于是

$$[K:F]=[K:K_1]\,[K_1:F]\mid(n-m)!\,m!.$$

而二项式系数 $\binom{n}{m}=n!/(m!(n-m)!)$ 是整数, 故 $m!(n-m)!\mid n!$, 从而 $[K:F]\mid n!$.
若 f 不可约, 取 f 在 K 中的一个根 α. 则 $[F(\alpha):F]=\deg f=n$, 且 $f=(x-\alpha)h$, 其中 h 在 $F(\alpha)$ 上次数为 $n-1$, K 是 h 在 $F(\alpha)$ 上的分裂域. 由归纳假设 $[K:F(\alpha)]\mid(n-1)!$, 故

$$[K:F]=[K:F(\alpha)]\,[F(\alpha):F]\mid(n-1)!\cdot n=n!.$$

归纳完成, 结论对所有 n 成立.

习题 3.2

Prove that the polynomial x^4+3x+3 is irreducible over the field $\mathbb{Q}[\sqrt[3]{2}]$.

解答

题目翻译: 证明多项式 x^4+3x+3 在域 $\mathbb{Q}[\sqrt[3]{2}]$ 上不可约.
解答: 同本作业习题 3.2, 解答见上.

习题 2.2

Let $f(x)=x^n-a_{n-1}x^{n-1}+\cdots\pm a_0$ be an irreducible polynomial over F, and let α be a root of f in an extension field K. Determine the element α^{-1} explicitly in terms of α and of the coefficients a_i.

解答

题目翻译: 设 $f(x)=x^n-a_{n-1}x^{n-1}+\cdots\pm a_0$ 是 F 上的不可约多项式, α 是 f 在扩域 K 中的一个根. 用 α 与系数 a_i 明确表示 α^{-1}.

解答: 按题设符号, 各项正负号交替, $f(x)=x^n-a_{n-1}x^{n-1}+a_{n-2}x^{n-2}-\cdots+(-1)^n a_0$. 因为 f 不可约且 α 是它的根, $a_0\neq 0$ (若 $a_0=0$ 则 $x\mid f$, 与不可约矛盾; 此时 $\alpha\neq 0$ 确可逆). 由 $f(\alpha)=0$,

$$\alpha^n-a_{n-1}\alpha^{n-1}+a_{n-2}\alpha^{n-2}-\cdots+(-1)^n a_0=0.$$

把除常数项以外的各项提出因子 α:

$$\alpha\Big(\alpha^{n-1}-a_{n-1}\alpha^{n-2}+a_{n-2}\alpha^{n-3}-\cdots+(-1)^{n-1}a_1\Big)=(-1)^{n+1}a_0.$$

两边除以 $(-1)^{n+1}a_0$ 得

$$\alpha^{-1}=\frac{\alpha^{n-1}-a_{n-1}\alpha^{n-2}+a_{n-2}\alpha^{n-3}-\cdots+(-1)^{n-1}a_1}{(-1)^{n+1}a_0}.$$

例如 $n=2$ 时 $f(x)=x^2-a_1x+a_0$, $\alpha^2-a_1\alpha+a_0=0$ 给出 $\alpha^{-1}=(a_1-\alpha)/a_0$, 与公式一致.

习题 3.3

Let $\zeta_n=\mathrm{e}^{2\pi\mathrm{i}/n}$. Prove that $\zeta_5\notin\mathbb{Q}(\zeta_7)$.

解答

题目翻译: 设 $\zeta_n=\mathrm{e}^{2\pi\mathrm{i}/n}$. 证明 $\zeta_5\notin\mathbb{Q}(\zeta_7)$.

解答: 利用分圆多项式的标准事实: n 次分圆多项式 $\Phi_n(x)$ 在 $\mathbb{Q}$ 上不可约, 故 $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$. 于是

$$[\mathbb{Q}(\zeta_5):\mathbb{Q}]=\varphi(5)=4,\qquad [\mathbb{Q}(\zeta_7):\mathbb{Q}]=\varphi(7)=6.$$

反设 $\zeta_5\in\mathbb{Q}(\zeta_7)$, 则 $\mathbb{Q}(\zeta_5)\subseteq\mathbb{Q}(\zeta_7)$, 由次数公式 $[\mathbb{Q}(\zeta_7):\mathbb{Q}]=[\mathbb{Q}(\zeta_7):\mathbb{Q}(\zeta_5)]\,[\mathbb{Q}(\zeta_5):\mathbb{Q}]$, 得 4 整除 6, 矛盾. 所以 $\zeta_5\notin\mathbb{Q}(\zeta_7)$.

习题 3.4

Let $\zeta_n = \mathrm{e}^{2\pi \mathrm{i}/n}$. Determine the irreducible polynomial over $\mathbb{Q}$ and over $\mathbb{Q}(\zeta_3)$ of (a) ζ_4, (b) ζ_6, (c) ζ_8, (d) ζ_9, (e) ζ_{10}, (f) ζ_{12}.

解答

题目翻译: 设 $\zeta_n = \mathrm{e}^{2\pi \mathrm{i}/n}$. 求 $\zeta_4, \zeta_6, \zeta_8, \zeta_9, \zeta_{10}, \zeta_{12}$ 分别在 $\mathbb{Q}$ 上与 $\mathbb{Q}(\zeta_3)$ 上的不可约多项式.

解答: 记 $\omega = \zeta_3 = \mathrm{e}^{2\pi \mathrm{i}/3}$, 则 $\omega^2 + \omega + 1 = 0$, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\mathrm{i}\sqrt{3})$, $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. 在 $\mathbb{Q}$ 上的不可约多项式就是分圆多项式 Φ_n.

(a) $\zeta_4 = \mathrm{i}$. 在 $\mathbb{Q}$ 上: $\Phi_4(x) = x^2 + 1$. 在 $\mathbb{Q}(\zeta_3)$ 上仍为 $x^2 + 1$: 反设 $\mathrm{i} \in \mathbb{Q}(\mathrm{i}\sqrt{3})$, 写 $\mathrm{i} = a + b\mathrm{i}\sqrt{3}$, $a, b \in \mathbb{Q}$, 比较实部与虚部得 $a = 0$, $b = \pm 1/\sqrt{3} \notin \mathbb{Q}$, 矛盾, 故 $x^2 + 1$ 在 $\mathbb{Q}(\zeta_3)$ 上无根, 从而不可约.

(b) $\zeta_6 = \mathrm{e}^{\pi \mathrm{i}/3} = 1 + \omega \in \mathbb{Q}(\zeta_3)$. 在 $\mathbb{Q}$ 上: $\Phi_6(x) = x^2 - x + 1$. 在 $\mathbb{Q}(\zeta_3)$ 上它属于基域, 极小多项式为 $x - \zeta_6$.

(c) ζ_8. 在 $\mathbb{Q}$ 上: $\Phi_8(x) = x^4 + 1$. 在 $\mathbb{Q}(\zeta_3)$ 上: 因为 $[\mathbb{Q}(\zeta_8, \zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \mathrm{i}, \sqrt{3}) : \mathbb{Q}] = 8$, 故 $[\mathbb{Q}(\zeta_8, \zeta_3) : \mathbb{Q}(\zeta_3)] = 4 = \deg \Phi_8$, Φ_8 保持不可约, 仍为 $x^4 + 1$.

(d) ζ_9. 在 $\mathbb{Q}$ 上: $\Phi_9(x) = (x^9 - 1)/(x^3 - 1) = x^6 + x^3 + 1$. 因 $\zeta_9^3 = \omega \in \mathbb{Q}(\zeta_3)$ 且 $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$, 故 $[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_3)] = 3$. ζ_9 是 $x^3 - \omega$ 的根, 该三次多项式无根于 $\mathbb{Q}(\zeta_3)$ (它的根 $\zeta_9, \zeta_9\omega, \zeta_9\omega^2$ 都不在 $\mathbb{Q}(\zeta_3)$ 中, 因 $[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\zeta_3)] = 3 > 1$), 故在 $\mathbb{Q}(\zeta_3)$ 上的极小多项式为 $x^3 - \zeta_3$.

(e) ζ_{10}. 在 $\mathbb{Q}$ 上: $\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1$. 因 $\mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5)$ 的唯一二次子域是 $\mathbb{Q}(\sqrt{5})$, 而 $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ 不在其中, 故 $[\mathbb{Q}(\zeta_{10}, \zeta_3) : \mathbb{Q}] = 8$, 从而 $[\mathbb{Q}(\zeta_{10}, \zeta_3) : \mathbb{Q}(\zeta_3)] = 4 = \deg \Phi_{10}$, 在 $\mathbb{Q}(\zeta_3)$ 上仍为 $x^4 - x^3 + x^2 - x + 1$.

(f) $\zeta_{12} = \mathrm{e}^{\pi \mathrm{i}/6}$. 在 $\mathbb{Q}$ 上: $\Phi_{12}(x) = x^4 - x^2 + 1$. 因 $\zeta_{12}^2 = \zeta_6 = 1 + \omega \in \mathbb{Q}(\zeta_3)$ 且 $\zeta_{12} \notin \mathbb{Q}(\zeta_3)$ (否则 $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3}, \mathrm{i})$ 将等于 $\mathbb{Q}(\sqrt{-3})$, 不可能), 故 $[\mathbb{Q}(\zeta_{12}) : \mathbb{Q}(\zeta_3)] = 2$, 在 $\mathbb{Q}(\zeta_3)$ 上的极小多项式为 $x^2 - \zeta_6 = x^2 - (1 + \zeta_3)$.

汇总如下表:

	$\mathbb{Q}$ 上	$\mathbb{Q}(\zeta_3)$ 上
ζ_4	$x^2 + 1$	$x^2 + 1$
ζ_6	$x^2 - x + 1$	$x - \zeta_6$
ζ_8	$x^4 + 1$	$x^4 + 1$
ζ_9	$x^6 + x^3 + 1$	$x^3 - \zeta_3$
ζ_{10}	$x^4 - x^3 + x^2 - x + 1$	$x^4 - x^3 + x^2 - x + 1$
ζ_{12}	$x^4 - x^2 + 1$	$x^2 - (1 + \zeta_3)$

习题 3.5

Determine the values of n such that ζ_n has degree at most 3 over $\mathbb{Q}$.

解答

题目翻译: 确定使 ζ_n 在 $\mathbb{Q}$ 上的次数至多为 3 的 n 的值.
解答:ζ_n 在 $\mathbb{Q}$ 上的次数为 $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$. 需要 $\varphi(n)\le 3$. 直接列出:

$$\varphi(1)=\varphi(2)=1,\qquad \varphi(3)=\varphi(4)=\varphi(6)=2.$$

且不存在 n 使 $\varphi(n)=3$ (对 $n>2$, $\varphi(n)$ 为偶数, 而 $n=1,2$ 时 φ 取 1; 标准结论: $\varphi(n)$ 为奇数当且仅当 $n=1,2$, 故 $\varphi(n)=3$ 无解). 又 $\varphi(5)=\varphi(8)=\varphi(10)=\varphi(12)=4>3$, $n\ge 5$ 时 $\varphi(n)$ 只会更大. 故所求为

$$n\in\{1,2,3,4,6\}.$$

习题 4.1

Let $K=\mathbb{Q}(\alpha)$, where α is a root of x^3-x-1. Determine the irreducible polynomial for $\gamma=1+\alpha^2$ over $\mathbb{Q}$.

解答

题目翻译: 设 $K=\mathbb{Q}(\alpha)$, 其中 α 是 x^3-x-1 的一个根. 求 $\gamma=1+\alpha^2$ 在 $\mathbb{Q}$ 上的不可约多项式.
解答:x^3-x-1 在 $\mathbb{Q}$ 上不可约 (有理根只可能是 ±1, 代入均不为 0), 故 $[K:\mathbb{Q}]=3$, 且由 $\alpha^3=\alpha+1$ 得 $\alpha^4=\alpha^2+\alpha$. 先证 $\gamma\notin\mathbb{Q}$: 若 $\gamma=1+\alpha^2\in\mathbb{Q}$, 则 $\alpha^2\in\mathbb{Q}$, 于是 α 满足次数不超过 2 的方程 $x^2-\alpha^2=0$, 与 $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ 矛盾. 故 $\deg\gamma\neq 1$. 又 $\deg\gamma$ 整除 $[K:\mathbb{Q}]=3$, 所以 $\deg\gamma=3$.
计算 γ 的幂. 利用 $\alpha^3=\alpha+1$, $\alpha^4=\alpha^2+\alpha$:

$$\gamma=1+\alpha^2,$$

$$\gamma^2=(1+\alpha^2)^2=1+2\alpha^2+\alpha^4=1+2\alpha^2+\alpha^2+\alpha=1+\alpha+3\alpha^2,$$

$$\gamma^3=\gamma\cdot\gamma^2=(1+\alpha^2)(1+\alpha+3\alpha^2)=1+\alpha+3\alpha^2+\alpha^2+\alpha^3+3\alpha^4=2+5\alpha+7\alpha^2,$$

其中 $1+\alpha+4\alpha^2+\alpha^3+3\alpha^4=1+\alpha+4\alpha^2+(\alpha+1)+3(\alpha^2+\alpha)=2+5\alpha+7\alpha^2$. 现在求 a,b,c 使 $\gamma^3=a\gamma^2+b\gamma+c$:

$$\gamma^3-a\gamma^2-b\gamma-c=(2-a-b-c)+(5-a)\alpha+(7-3a-b)\alpha^2,$$

比较 $\{1, \alpha, \alpha^2\}$ 的系数, 得 $a = 5, b = -8, c = 5$. 故 γ 满足

$$\gamma^3 - 5\gamma^2 + 8\gamma - 5 = 0.$$

多项式 $x^3 - 5x^2 + 8x - 5$ 首一次数为 3 且以 γ 为根, 正是 γ 的极小多项式. 也可直接检验其不可约: 有理根 $\pm 1, \pm 5$ 代入均不为 0.

习题 7.11

Let $f = ax^2 + bx + c$ with a, b, c in a ring R. Show that the ideal of the polynomial ring $R[x]$ that is generated by f and f' contains the discriminant, the constant polynomial $b^2 - 4ac$.

解答

题目翻译: 设 $f = ax^2 + bx + c$, 其中 a, b, c 属于环 R. 证明多项式环 $R[x]$ 中由 f 与 f' 生成的理想包含判别式, 即常数多项式 $b^2 - 4ac$.

解答: f 的导数为 $f' = 2ax + b$. 记理想 $I = (f, f') \subseteq R[x]$, 则 $f' \in I$ 蕴含 $(f')^2 \in I$, $f \in I$ 蕴含 $4af \in I$. 直接展开:

$$(f')^2 = (2ax + b)^2 = 4a^2x^2 + 4abx + b^2, \qquad 4af = 4a^2x^2 + 4abx + 4ac.$$

相减得

$$(f')^2 - 4af = b^2 - 4ac.$$

左端是 I 中两个元素之差, 仍属于 I. 所以判别式 $b^2 - 4ac \in I = (f, f')$.

习题 7.7

Let K be a finite field. Prove that the product of the nonzero elements of K is -1.

解答

题目翻译: 设 K 是有限域. 证明 K 中所有非零元素的乘积等于 -1.

解答: 设 $|K| = q$, 则 $K^\times$ 是 $q - 1$ 阶乘法群. 由 Lagrange 定理, 每个非零元素 a 都满足 $a^{q-1} = 1$, 即 a 是 $x^{q-1} - 1$ 的根. 域中多项式 $x^{q-1} - 1$ 至多有 $q - 1$ 个根, 而 $K^\times$ 恰有 $q - 1$ 个元素, 所以 $x^{q-1} - 1$ 的根恰好就是 $K^\times$ 的全部元素:

$$x^{q-1} - 1 = \prod_{a \in K^\times} (x - a).$$

比较常数项: 左端常数项为 -1, 右端常数项为 $(-1)^{q-1}\prod_{a\in K^\times} a$. 故

$$\prod_{a\in K^\times} a = \frac{-1}{(-1)^{q-1}} = (-1)^q.$$

当 q 为奇数时 $(-1)^q = -1$; 当 q 为 2 的幂时 K 的特征为 2, 此时 $(-1)^q = 1 = -1$. 两种情形下都有 $\prod_{a\in K^\times} a = -1$.

习题 7.12

Let p be a prime integer, and let $q = p^r$ and $q' = p^k$. For which values of r and k does $x^{q'} - x$ divide $x^q - x$ in $\mathbb{Z}[x]$?

解答

题目翻译: 设 p 是素数, $q = p^r$, $q' = p^k$. 问 r 与 k 取何值时 $x^{q'} - x$ 在 $\mathbb{Z}[x]$ 中整除 $x^q - x$?

解答: 答案是: 当且仅当 $k \mid r$.

充分性: 设 $r = kt$. 记 $u = x^{p^k}$, 则 $x^{p^r} = (x^{p^k})^{p^{k(t-1)}} = u^{p^{k(t-1)}}$. 用因式分解 $u^m - x = (u-x)(u^{m-1} + u^{m-2}x + \cdots + x^{m-1})$, 取 $m = p^{k(t-1)}$, 得 $u - x = x^{p^k} - x$ 整除 $u^m - x = x^{p^r} - x$. 分解式的第二个因子是整系数多项式, 故整除关系在 $\mathbb{Z}[x]$ 中成立.

必要性: 若 $x^{p^k} - x \mid x^{p^r} - x$ 在 $\mathbb{Z}[x]$ 中成立, 则模 p 后在 $\mathbb{F}_p[x]$ 中 $x^{p^k} - x \mid x^{p^r} - x$. 多项式 $x^{p^m} - x$ 在 $\mathbb{F}_p$ 的代数闭包中无重根 (其导数 $p^m x^{p^m-1} - 1 = -1 \neq 0$), 且它的根恰为 $\mathbb{F}_{p^m}$ 的全部元素 ($\mathbb{F}_{p^m}$ 中每个元素满足 $x^{p^m} = x$, 而这样的元素至多 p^m 个). 因此 $x^{p^k} - x \mid x^{p^r} - x$ 蕴含 $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^r}$. 有限域的子域判定是: $\mathbb{F}_{p^k}$ 含于 $\mathbb{F}_{p^r}$ 当且仅当 $k \mid r$ (因为 $\mathbb{F}_{p^r}$ 是 $x^{p^r} - x$ 在 $\mathbb{F}_p$ 上的分裂域, 其子域对应 r 的因数). 故 $k \mid r$.

综上, $x^{p^k} - x$ 在 $\mathbb{Z}[x]$ 中整除 $x^{p^r} - x$ 当且仅当 $k \mid r$.

习题 8.1

Prove that every finite extension of a finite field has a primitive element.

解答

题目翻译: 证明有限域的每个有限扩张都有本原元素.

解答: 设 F 是有限域, K/F 是有限扩张. 则 $[K:F]$ 有限且 F 有限, 所以 K 是有限集, 是有限域. 由习题 7.13 (域乘法群的有限子群是循环群), $K^\times$ 是循环群. 取 $K^\times$ 的生成元 α, 则 $K^\times = \langle\alpha\rangle$. 于是 K 的每个非零元都是 α 的幂, 而 $0 = 0 \in F$, 所以 $K = F(\alpha)$. 因此 α 是 K/F 的本原元素.

5

第五次作业

习题 7.1

Let $G = D_4$ be the dihedral group of symmetries of the square.
(a) What is the stabilizer of a vertex? of an edge?
(b) G operates on the set of two elements consisting of the diagonal lines. What is the stabilizer of a diagonal?

解答 习题 7.1

题目翻译: 设 $G = D_4$ 是正方形的对称群. (a) 一个顶点的稳定子是什么? 一条边呢? (b) G 作用在由两条对角线组成的二元集合上. 一条对角线的稳定子是什么?
解答:(a) 正方形有 4 个顶点, 而 D_4 作用在顶点集上传递, 故一个顶点 v 的轨道长度为 4. 由轨道-稳定子定理 (有限群作用中, 轨道长度等于 $|G|$ 除以稳定子阶数), $|G_v| = |D_4|/4 = 8/4 = 2$. 保持 v 不动的元素是恒等变换与关于过 v 及其对顶点的对角线的反射, 故稳定子为 $\{1, $关于该对角线的反射$\}$. 同理, 正方形有 4 条边, 边的轨道长度为 4, 故边的稳定子阶数也为 2, 由恒等变换与关于过该边中点及其对边中点的直线的反射组成.
(b) 两条对角线在 G 作用下构成一条轨道 (旋转 90 度即可把一条对角线送到另一条), 轨道长度为 2. 由轨道-稳定子定理, 一条对角线 d 的稳定子阶数为 $8/2 = 4$. 保持 d 不变的元素是: 恒等变换, 旋转 180 度的旋转 (把两条对角线分别映到自身), 关于 d 的反射, 以及关于另一条对角线的反射. 故稳定子为

$$\{1,\ r^2,\ \text{关于}d\ \text{的反射},\ \text{关于另一条对角线的反射}\},$$

它是一个 4 阶子群.

习题 7.5

Let G be the group of symmetries of a cube, including the orientation-reversing symmetries. Describe the elements of G geometrically.

解答 习题 7.5

题目翻译: 设 G 是立方体的对称群, 包括反转定向的对称. 用几何语言描述 G 的元素.
解答:G 是保持立方体的所有等距变换, 阶数为 48. 它由两部分组成.
保持定向的旋转有 24 个: 恒等变换 1 个; 绕通过一对相对面中心的轴的旋转, 轴有 3

条, 每条轴给出 90 度, 180 度, 270 度三个非平凡旋转, 共 9 个; 绕通过一对相对顶点的体对角线的旋转, 轴有 4 条, 每条轴给出 120 度, 240 度两个非平凡旋转, 共 8 个; 绕通过一对相对棱的中点的轴的 180 度旋转, 轴有 6 条, 共 6 个. 合计 $1+9+8+6=24$. 反转定向的对称也有 24 个. 记 ι 为中心反演, 即把每个点 x 映到其对径点 $-x$ 的等距变换. ι 与所有等距变换交换且反转定向. 每个反转定向的对称可唯一写成 ι 与某个旋转的复合, 其中包含: 关于过立方体中心且平行于某个面的平面的反射 (共 3 个), 关于过中心且含一对相对棱的平面的反射 (共 6 个), 其余 15 个是先作旋转再作中心反演的旋转反演 (rotoreflection). 因而 G 的阶数为 $24+24=48$.
旋转群同构于 S_4 (它传递地作用在四条体对角线上, 诱导出 S_4), 而 ι 生成 2 阶中心子群, 故 $G \cong S_4 \times C_2$.

习题 7.10

(a) Describe the orbit and the stabilizer of the matrix $\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$ under conjugation in the general linear group $\mathrm{GL}_n(\mathbb{R})$. (b) Interpreting the matrix in $\mathrm{GL}_2(\mathbb{F}_5)$, find the order of the orbit.

解答　习题 7.10

题目翻译:(a) 在一般线性群 $\mathrm{GL}_n(\mathbb{R})$ 中, 描述矩阵 $\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$ 在共轭作用下的轨道与稳定子. (b) 把该矩阵解释为 $\mathrm{GL}_2(\mathbb{F}_5)$ 中的矩阵, 求其轨道的阶.
解答:(a) 该矩阵是 2 阶方阵, 故所属的一般线性群为 $\mathrm{GL}_2(\mathbb{R})$, 即此处 $n=2$. 记 $A=\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$. A 的特征值为 1 和 2, 互异, 故 A 可对角化, 且与之相似的矩阵恰为特征值为 1, 2 的矩阵, 即迹为 3, 行列式为 2 的矩阵. 因此轨道为

$$\{B \in \mathrm{GL}_2(\mathbb{R}) : \operatorname{tr} B = 3,\ \det B = 2\} = \{PAP^{-1} : P \in \mathrm{GL}_2(\mathbb{R})\}.$$

稳定子 $\{P : PA = AP\}$: 设 $P=\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]$, 则 $PA=\left[\begin{smallmatrix}a&2b\\c&2d\end{smallmatrix}\right]$, $AP=\left[\begin{smallmatrix}a&b\\2c&2d\end{smallmatrix}\right]$, 比较得 $b=0$, $c=0$. 故稳定子为非零对角矩阵 $\{\left[\begin{smallmatrix}a&0\\0&d\end{smallmatrix}\right] : a,d \neq 0\} \cong \mathbb{R}^* \times \mathbb{R}^*$.
(b) 在 $\mathrm{GL}_2(\mathbb{F}_5)$ 中, A 的稳定子仍为非零对角矩阵 (因 $1 \neq 2$ 于 $\mathbb{F}_5$), 其阶数为 $(5-1)^2=16$. 又 $|\mathrm{GL}_2(\mathbb{F}_5)| = (5^2-1)(5^2-5) = 24 \times 20 = 480$. 由轨道-稳定子定理, 轨道阶数为 $480/16 = 30$.

习题 8.4

Let H be the stabilizer of the index 1 for the operation of the symmetric group $G = S_n$ on the set of indices $\{1, \ldots, n\}$. Describe the left cosets of H in G and the map (6.8.4) in this case.

解答　习题 8.4

题目翻译: 设 H 是对称群 $G = S_n$ 作用在指标集 $\{1, \ldots, n\}$ 上时指标 1 的稳定子. 描述 H 在 G 中的左陪集, 以及此时的映射 (6.8.4).

解答: $H = \{\sigma \in S_n : \sigma(1) = 1\} \cong S_{n-1}$, 即固定指标 1 的置换全体. 对任意 $g \in S_n$, 左陪集 $gH = \{g\sigma : \sigma \text{ 固定1}\}$. 因为 $(g\sigma)(1) = g(1)$, gH 中每个置换都把 1 映到 $g(1)$. 反之, 若置换 τ 满足 $\tau(1) = g(1)$, 则 $g^{-1}\tau$ 固定 1, 故 $\tau \in gH$. 因此

$$gH = \{\tau \in S_n : \tau(1) = g(1)\},$$

即 gH 恰为所有把 1 映到 $i = g(1)$ 的置换组成的集合. 于是左陪集与指标一一对应, 共有 n 个左陪集, $[S_n : H] = n$.

映射 (6.8.4) 是轨道-稳定子定理中的双射 $\varphi : G/H \to G(1)$, $gH \mapsto g \cdot 1 = g(1)$. 在此情形下

$$\varphi : \{gH : g \in S_n\} \to \{1, \ldots, n\}, \qquad gH \mapsto g(1),$$

它把每个左陪集送到该陪集把 1 映到的那个指标. 这是良定义的双射: $g_1H = g_2H$ 当且仅当 $g_1(1) = g_2(1)$, 且对每个 i 都存在把 1 映到 i 的置换.

习题 9.3

Determine the order of the group of symmetries of a dodecahedron, when orientation-reversing symmetries such as reflections in planes are allowed.

解答　习题 9.3

题目翻译: 在允许平面反射等反转定向的对称时, 求正十二面体的对称群的阶.

解答: 正十二面体有 12 个正五边形面, 其全对称群 (含反转定向) 传递地作用在这 12 个面上. 固定一个面 f 的对称必把正五边形面 f 映到自身, 诱导出该正五边形的对称群, 即 10 阶二面体群 D_5 (5 个旋转与 5 个反射). 反过来, D_5 中每个对称都能由正十二面体的一个整体对称实现, 故 f 的稳定子阶数为 10. 由轨道-稳定子定理, 全对称群阶数为 $12 \times 10 = 120$.

(作为对照, 正十二面体的旋转群阶数为 60, 同构于 A_5; 加入反转定向使阶数加倍, 全对称群同构于 $A_5 \times C_2$.)

习题 10.2

Let S be a finite set on which a group G operates transitively, and let U be a subset of S. Prove that the subsets gU cover S evenly, that is, that every element of S is in the same number of sets gU .

解答　习题 10.2

题目翻译: 设 G 传递地作用在有限集 S 上, U 是 S 的一个子集. 证明子集 gU $(g \in G)$ 均匀地覆盖 S, 即 S 中每个元素属于同样多个集合 gU.

解答: 对固定的 $s \in S$, 记 $N(s) = \#\{g \in G : s \in gU\}$, 即含 s 的集合 gU 的个数. 要证 $N(s)$ 与 s 无关.

计数集合 $P = \{(g, u) \in G \times U : gu = s\}$ 的基数. 一方面, 固定 $u \in U$: 因作用传递, 存在 h 使 $hu = s$; 于是 $gu = s$ 当且仅当 $h^{-1}g \in G_u$, 故满足条件的 g 恰为 hG_u, 个数为 $|G_u|$. 同一轨道上各点的稳定子彼此共轭, 故 $|G_u| = |G_s|$. 于是 $|P| = |U| \cdot |G_s|$. 另一方面, 固定 $g \in G$: 满足 $gu = s$ 的 $u \in U$ 至多一个 (若 $g^{-1}s \in U$ 则为 $u = g^{-1}s$, 否则没有), 故 $|P| = N(s)$.

所以 $N(s) = |U| \cdot |G_s|$, 因传递作用使 $|G_s|$ 与 s 无关, $N(s)$ 与 s 无关. 即每个元素恰好属于 $|U| \cdot |G_s|$ 个集合 gU, 覆盖是均匀的.

习题 10.3

Consider the operation of left multiplication by G on the set of its subsets. Let U be a subset such that the sets gU partition G. Let H be the unique subset in this orbit that contains 1. Prove that H is a subgroup of G.

解答　习题 10.3

题目翻译: 考虑 G 通过左乘作用在自身的所有子集组成的集合上. 设 U 是一个子集, 使得集合 gU $(g \in G)$ 构成 G 的一个划分. 设 H 是这条轨道中唯一含 1 的那个子集. 证明 H 是 G 的子群.

解答: 轨道 $\{gU : g \in G\}$ 划分 G, 且 H 是其中唯一含 1 的子集. 先证: 对任意 $a \in H$, 有 $a^{-1}H = H$. 事实上 $a^{-1}H = a^{-1}(g_0U)$ 仍形如某 gU, 故在同一轨道中; 又 $a \in H$, 故 $1 = a^{-1}a \in a^{-1}H$, 即 $a^{-1}H$ 也是轨道中含 1 的子集. 由唯一性, $a^{-1}H = H$.

于是对任意 $a, b \in H$, $a^{-1}b \in H$. 取 $b = 1$ 得 $a^{-1} \in H$; 又因 $a^{-1} \in H$, 把 a^{-1} 当作上述论断中的第一个元素, 得 $(a^{-1})^{-1}b = ab \in H$. 故 H 含 1, 对乘法封闭, 且每个元素在 H 中有逆元, 所以 $H \leq G$.

习题 11.1

Describe all ways in which S_3 can operate on a set of four elements.

解答　习题 11.1

题目翻译: 描述 S_3 作用在四个元素的集合上的所有方式.

解答: 一个作用等价于一个同态 $\varphi : S_3 \to S_4$ (四个元素上的置换群). S_3 的正规子群只有 $\{1\}$, A_3, S_3 三个, 故像 $\varphi(S_3) \cong S_3/\ker\varphi$ 同构于 S_3, C_2 或 $\{1\}$. 分三种情形.

(1) 平凡作用, $\ker\varphi = S_3$: 每个元素都映为恒等, 四个元素全部固定.

(2) $\ker\varphi = A_3$, 像为 2 阶子群: φ 是自然同态 $S_3 \to S_3/A_3 \cong C_2$ 再嵌入 S_4, 偶置换

映为恒等, 奇置换 (3 个对换) 都映为同一个二阶元素. S_4 中的二阶元素有两类: 一个对换 (交换两个元素, 固定另两个), 或两个不交对换之积 (把四个元素分成两对分别交换). 这两类分别给出一种作用, 其轨道分解为 $1+1+2$ 或 $2+2$.
(3) 忠实作用, $\ker\varphi=\{1\}$, 像 $\cong S_3$: 像必须是 S_4 的一个 6 阶子群. S_4 中同构于 S_3 的子群恰是单点稳定子, 共 4 个. 作用不可能传递 (轨道长度 4 不整除 $|S_3|=6$), 也不可能有 2 元素轨道 (否则 $S_3\to S_2$ 的核至少含 A_3, 不忠实), 故四个元素中恰有一个被所有置换固定, S_3 作为全体置换忠实作用在其余三个元素上, 轨道分解为 $1+3$. 选取固定的那个元素有 4 种可能, 在重新编号的意义下这是唯一一类忠实作用.
因此 S_3 在四元素集上的作用分为: 平凡作用, 两类 2 阶像的作用, 以及一类 (含 4 个彼此等价的) 忠实作用.

习题 11.6

Let $F=\mathbb{F}_3$. There are four one-dimensional subspaces of the space of column vectors F^2. List them. Left multiplication by an invertible matrix permutes these subspaces. Prove that this operation defines a homomorphism $\varphi:\mathrm{GL}_2(F)\to S_4$. Determine the kernel and image of this homomorphism.

解答 习题 11.6

题目翻译: 设 $F=\mathbb{F}_3$. 二维列向量空间 F^2 有四个一维子空间, 把它们列出来. 用可逆矩阵左乘会置换这些子空间. 证明这一作用定义了同态 $\varphi:\mathrm{GL}_2(F)\to S_4$, 并确定这个同态的核与像.
解答:F^2 的非零向量共 $3^2-1=8$ 个, 每个一维子空间含 $3-1=2$ 个非零向量, 且非零向量的非零标量倍张成同一个子空间, 故一维子空间数为 $8/2=4$. 取代表元, 四个子空间为

$$L_1=\left\langle\begin{bmatrix}1\\0\end{bmatrix}\right\rangle,\quad L_2=\left\langle\begin{bmatrix}0\\1\end{bmatrix}\right\rangle,\quad L_3=\left\langle\begin{bmatrix}1\\1\end{bmatrix}\right\rangle,\quad L_4=\left\langle\begin{bmatrix}1\\2\end{bmatrix}\right\rangle.$$

即 x 轴, y 轴, 以及斜率分别为 1 和 2 的两条直线.
对 $A\in\mathrm{GL}_2(F)$, 左乘把子空间 L 送到 $AL=\{Av:v\in L\}$, 仍是一维子空间, 且 A 是 F^2 的线性双射, 故给出四个子空间的一个置换. 由 $(AB)L=A(BL)$ 与 $IL=L$, 该作用定义同态 $\varphi:\mathrm{GL}_2(F_3)\to S_4$.
核: A 保持每个一维子空间当且仅当每个非零向量都是 A 的特征向量, 这当且仅当 A 是纯量矩阵 λI ($\lambda\in\mathbb{F}_3^*$). 故 $\ker\varphi=\{I,2I\}\cong C_2$.
像: $|\mathrm{GL}_2(\mathbb{F}_3)|=(3^2-1)(3^2-3)=8\times6=48$. 由同态基本定理, $|\operatorname{im}\varphi|=48/2=24=|S_4|$, 故 $\operatorname{im}\varphi=S_4$, 即 φ 是满射, 从而 $\mathrm{GL}_2(\mathbb{F}_3)/\{\pm I\}\cong S_4$.

习题 12.1

Explain why the groups of symmetries of the dodecahedron and the icosahedron are isomorphic.

解答 习题 12.1

题目翻译: 解释为什么正十二面体和正二十面体的对称群同构.
解答: 正二十面体是正十二面体的对偶多面体, 反之亦然: 正十二面体有 12 个正五边形面, 各面的中心恰构成一个正二十面体的 12 个顶点; 正二十面体有 20 个三角形面, 各面的中心构成正十二面体的 20 个顶点.
取对偶的过程与所有等距变换相容. 若 g 是保持正十二面体的一个等距变换, 则 g 把面映到面, 因而把面的中心映到面的中心, 于是 g 把以这些面中心为顶点的正二十面体保持, 给出正二十面体的一个对称. 反过来, 每个正二十面体的对称也保持其面中心, 从而给出正十二面体的对称. 这两个对应互逆且保持复合, 故两个对称群同构 (无论只取旋转群还是取全对称群都一样).

习题 12.3

Let O be the group of rotations of a cube, and let S be the set of four diagonal lines connecting opposite vertices. Determine the stabilizer of one of the diagonals.

解答 习题 12.3

题目翻译: 设 O 是立方体的旋转群, S 是连接相对顶点的四条体对角线组成的集合. 求其中一条体对角线的稳定子.
解答: 立方体的旋转群 O 阶数为 24, 它传递地作用在四条体对角线上 (例如绕面心轴旋转即可把任一体对角线送到任一另一条). 由轨道-稳定子定理, 一条体对角线 d 的稳定子阶数为 $24/4 = 6$. 具体地, 保持 d 的旋转有两类: (1) 绕 d 自身的旋转: 恒等, 120 度, 240 度, 共 3 个, 它们分别固定 d 的两个端点; (2) 绕与 d 垂直的轴的 180 度旋转: 这样的轴有 3 条, 每条通过一对相对棱的中点, 该旋转交换 d 的两个端点, 共 3 个. 故稳定子共有 6 个元素. 它传递地作用在其余三条体对角线上, 同构于对称群 S_3.

习题 12.5

Prove that the icosahedral group has a subgroup of order 10.

解答 习题 12.5

题目翻译: 证明正二十面体群有一个 10 阶子群.
解答: 正二十面体群即正二十面体的旋转群, 阶数为 60. 正二十面体有 12 个顶点, 分成 6 对相对顶点, 每对相对顶点确定一条过中心的轴. 旋转群传递地作用在这 6 条轴上 (所有顶点彼此等价, 故任一条轴可映到任另一条). 固定一条轴 d 的旋转构成该轴的稳定子, 由轨道-稳定子定理其阶数为 $60/6 = 10$, 这就是一个 10 阶子群. 具体地, 它

由绕 d 的 5 个旋转 (角度 $0, 72, 144, 216, 288$ 度) 与交换 d 两端点的 5 个 180 度旋转组成, 同构于二面体群 D_5.

习题 2.1

Determine the centralizer and the order of the conjugacy class of (a) the matrix $\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]$ in $\mathrm{GL}_2(\mathbb{F}_3)$, (b) the matrix $\left[\begin{smallmatrix}1&1\\2&2\end{smallmatrix}\right]$ in $\mathrm{GL}_2(\mathbb{F}_5)$.

解答 习题 2.1

题目翻译: 求下列矩阵的中心化子与共轭类的阶: (a) 矩阵 $\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]$ 在 $\mathrm{GL}_2(\mathbb{F}_3)$ 中; (b) 矩阵 $\left[\begin{smallmatrix}1&1\\2&2\end{smallmatrix}\right]$ 在 $\mathrm{GL}_2(\mathbb{F}_5)$ 中.

解答: 两个矩阵的行列式都是 0, 本身不是可逆矩阵. 但共轭作用 $X \mapsto PXP^{-1}$ ($P \in \mathrm{GL}_2(F)$) 对全体 2×2 矩阵都有定义, 故中心化子指 $\mathrm{GL}_2(F)$ 中与给定矩阵可交换的矩阵, 共轭类指轨道 $\{PXP^{-1} : P \in \mathrm{GL}_2(F)\}$. 由轨道-稳定子定理, 共轭类的阶 $= |\mathrm{GL}_2(F)|/|$中心化子$|$.

(a) $A = \left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]$, 特征多项式 $x^2 - 2x = x(x-2)$, 特征值 $0, 2$ 互异, 故 A 与 $\left[\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right]$ 相似. 设 $P = \left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]$ 与 A 可交换: $PA = \left[\begin{smallmatrix}a+c&b+d\\a+c&b+d\end{smallmatrix}\right]$, $AP = \left[\begin{smallmatrix}a+b&a+b\\c+d&c+d\end{smallmatrix}\right]$, 比较得 $b = c$, $a = d$. 故 $P = \left[\begin{smallmatrix}a&b\\b&a\end{smallmatrix}\right] = aI + bJ$, 其中 $J = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$, $a, b \in \mathbb{F}_3$. 可逆条件 $\det P = a^2 - b^2 = (a-b)(a+b) \neq 0$, 即 $a \neq \pm b$. 满足条件的 (a, b) 有 4 个: $(1,0), (2,0), (0,1), (0,2)$. 故中心化子 $\{I, 2I, J, 2J\} \cong V_4$, 阶数为 4. 共轭类阶数 $= 48/4 = 12$.

(b) $B = \left[\begin{smallmatrix}1&1\\2&2\end{smallmatrix}\right]$, 特征多项式 $x^2 - 3x = x(x-3)$, 特征值 $0, 3$ 互异于 $\mathbb{F}_5$, 故与 $\left[\begin{smallmatrix}0&0\\0&3\end{smallmatrix}\right]$ 相似. 设 $P = \left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]$ 与 B 可交换: $PB = \left[\begin{smallmatrix}a+2b&a+2b\\c+2d&c+2d\end{smallmatrix}\right]$, $BP = \left[\begin{smallmatrix}a+c&b+d\\2a+2c&2b+2d\end{smallmatrix}\right]$, 比较得 $c = 2b$, $d = a + b$. 故 $P = \left[\begin{smallmatrix}a&b\\2b&a+b\end{smallmatrix}\right]$, $a, b \in \mathbb{F}_5$. 可逆条件 $\det P = a^2 + ab - 2b^2 \neq 0$. 当 $b = 0$ 时 $\det P = a^2 \neq 0$, 得 $a \in \{1, 2, 3, 4\}$, 共 4 个; 当 $b \neq 0$ 时令 $t = a/b$, $\det P = b^2(t^2 + t - 2) = b^2(t+2)(t-1) \neq 0$, 即 $t \notin \{1, 3\}$, 对每个 $b \in \mathbb{F}_5^*$ 有 3 个 t, 共 $4 \times 3 = 12$ 个. 故中心化子阶数为 $4 + 12 = 16$. 共轭类阶数 $= 480/16 = 30$.

习题 2.3

A group G of order 12 contains a conjugacy class of order 4. Prove that the center of G is trivial.

解答 习题 2.3

题目翻译: 一个 12 阶群 G 含有一个 4 阶共轭类. 证明 G 的中心平凡.

解答: 设 x 的共轭类有 4 个元素. 共轭类大小等于中心化子的指标 (轨道-稳定子定理), 故 $|C_G(x)| = 12/4 = 3$. 中心 $Z(G) \subseteq C_G(x)$ (中心元素与一切元素可交换), 故 $|Z(G)|$ 整除 3, 即 $|Z(G)| \in \{1, 3\}$.

若 $|Z(G)| = 3$, 则 $Z(G) = C_G(x)$. 但 x 总与自身可交换, 故 $x \in C_G(x) = Z(G)$, 于是 x 的共轭类只有 1 个元素, 与它有 4 个元素矛盾. 故 $|Z(G)| = 1$, 中心平凡.

习题 2.8

Determine the possible class equations of nonabelian groups of order 8.

解答 习题 2.8

题目翻译: 求 8 阶非交换群所有可能的类方程.
解答: 设 G 是 8 阶非交换群. 类方程中每一项是共轭类大小, 都整除 $|G| = 8$; 非中心类的共轭类大小大于 1, 故只可能为 2 或 4.
中心 $|Z(G)|$ 整除 8. 有限 p-群的中心非平凡, 故 $|Z(G)| \geq 2$; 又 G 非交换, $|Z(G)| \neq 8$. 若 $|Z(G)| = 4$, 则 $|G/Z(G)| = 2$, 循环群 $G/Z(G)$ 迫使 G 交换, 矛盾. 故 $|Z(G)| = 2$. 剩下的 $8 - 2 = 6$ 由若干大小为 2 或 4 的共轭类相加. 若有大小为 4 的共轭类, 设其代表元为 x, 则 $|C_G(x)| = 8/4 = 2 = |Z(G)|$, 故 $C_G(x) = Z(G)$; 但 $x \in C_G(x)$, 得 $x \in Z(G)$, 与类大小为 4 矛盾. 故不存在 4 阶共轭类, 只能是三个 2 阶共轭类.
因此非交换 8 阶群的类方程必为 $1 + 1 + 2 + 2 + 2$. (二面体群 D_4 与四元数群 Q_8 都实现这一方程.)

习题 2.13

Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and that $|G|$ is an odd integer. Prove that N is contained in the center of G.

解答 习题 2.13

题目翻译: 设 N 是群 G 的正规子群, $|N| = 5$ 且 $|G|$ 是奇数. 证明 N 含于 G 的中心.
解答:N 正规, 故共轭作用 $g \mapsto gng^{-1}$ 保持 N, 给出同态 $\varphi : G \to \mathrm{Aut}(N)$. 由于 $N \cong C_5$ 且 $\mathrm{Aut}(C_5) \cong (\mathbb{Z}/5)^\times \cong C_4$, 有 $|\mathrm{Aut}(N)| = 4$, 故 $|\varphi(G)|$ 整除 4.
另一方面, $\ker\varphi = C_G(N) = \{g : gn = ng \ \forall n \in N\} \supseteq N$. 由同态基本定理, $|G/C_G(N)| = |\varphi(G)|$ 整除 4. 因 $|G|$ 是奇数, 其因子 $|C_G(N)|$ 与商 $|G|/|C_G(N)|$ 都是奇数. 奇数又整除 4 者只能是 1, 故 $|G/C_G(N)| = 1$, 即 $C_G(N) = G$. 于是每个 $g \in G$ 与 N 中所有元素可交换, $N \subseteq Z(G)$.

习题 2.16

Let $\varphi : G \to G'$ be a surjective group homomorphism, let C denote the conjugacy class of an element x of G, and let C' denote the conjugacy class in G' of its image $\varphi(x)$. Prove that φ maps C surjectively to C', and that $|C'|$ divides $|C|$.

解答 习题 2.16

题目翻译: 设 $\varphi : G \to G'$ 是满的群同态, C 是 G 中元素 x 的共轭类, C' 是 G' 中 $\varphi(x)$ 的共轭类. 证明 φ 把 C 满射到 C', 且 $|C'|$ 整除 $|C|$.
解答: 满射性: 任取 $y' \in C'$, 存在 $g' \in G'$ 使 $y' = g'\varphi(x)g'^{-1}$. 因 φ 满, 取 $g \in G$ 使

$\varphi(g)=g'$. 则

$$y'=\varphi(g)\varphi(x)\varphi(g)^{-1}=\varphi(gxg^{-1}),$$

而 $gxg^{-1}\in C$, 故 $y'\in\varphi(C)$. 所以 $\varphi(C)=C'$.
整除性: $|C|=|G|/|C_G(x)|$, $|C'|=|G'|/|C_{G'}(\varphi(x))|$. 记 $K=\ker\varphi$, $H=\varphi^{-1}(C_{G'}(\varphi(x)))$. 则 $H\le G$ 且 $C_G(x)\subseteq H$ (若 g 与 x 可交换, 则 $\varphi(g)$ 与 $\varphi(x)$ 可交换). 又 φ 把 H 满射到 $C_{G'}(\varphi(x))$, 核为 K, 故 $|H|=|K|\cdot|C_{G'}(\varphi(x))|$. 由 $|G|=|K|\cdot|G'|$ 得

$$|C|=\frac{|G|}{|C_G(x)|}=\frac{|K||G'|}{|C_G(x)|}=|C'|\cdot\frac{|K|\,|C_{G'}(\varphi(x))|}{|C_G(x)|}=|C'|\cdot\frac{|H|}{|C_G(x)|}=|C'|\cdot[H:C_G(x)].$$

因 $[H:C_G(x)]$ 是整数, $|C'|$ 整除 $|C|$.

习题 1.1(e)

Determine the orbit of the polynomial below. If the polynomial is symmetric, write it in terms of the elementary symmetric functions. (e) $u_1^3+u_2^3+\cdots+u_n^3$.

解答　习题 1.1(e)

题目翻译: 求下列多项式的轨道. 若多项式是对称的, 把它写成初等对称函数的多项式. (e) $u_1^3+u_2^3+\cdots+u_n^3$.
解答: 记 $p=u_1^3+\cdots+u_n^3$. 对任意置换 $\sigma\in S_n$, 置换变量只是重新排列各项, p 不变, 故 p 是对称多项式, 其轨道只有一个元素, 即 $\{p\}$ 本身.
用初等对称函数表示. 令 $w_k=u_1^k+\cdots+u_n^k$, 记 $s_1=u_1+\cdots+u_n$, $s_2=\sum_{i<j}u_iu_j$, $s_3=\sum_{i<j<k}u_iu_ju_k$. 由 Newton 恒等式 $(w_k-s_1w_{k-1}+\cdots+(-1)^k ks_k=0)$ 取 $k=1,2,3$ 得

$$w_1=s_1,\qquad w_2=s_1w_1-2s_2=s_1^2-2s_2,\qquad w_3=s_1w_2-s_2w_1+3s_3.$$

代入得

$$p=w_3=s_1(s_1^2-2s_2)-s_2s_1+3s_3=s_1^3-3s_1s_2+3s_3.$$

习题 2.5

Use the systematic method on the discriminant in four variables, to determine the coefficients in $\Delta(s_1,\dots,s_4)$ of all monomials not divisible by s_4.

解答　习题 2.5

题目翻译: 对四变量判别式使用系统方法, 求出 $\Delta(s_1,\dots,s_4)$ 中所有不被 s_4 整除的单项式的系数.
解答: 四变量判别式 $\Delta=\prod_{i<j}(u_i-u_j)^2$ 是对称的齐次多项式, 次数为 $2\times\binom{4}{2}=12$; 写成 s_1,s_2,s_3,s_4 的多项式后, 每个单项式 $s_1^as_2^bs_3^cs_4^d$ 满足 $a+2b+3c+4d=12$. 不含

s_4 的项正是令 $s_4 = 0$ 所得 $\Delta(s_1, s_2, s_3, 0)$, 即多项式

$$x^4 - s_1x^3 + s_2x^2 - s_3x = x\left(x^3 - s_1x^2 + s_2x - s_3\right)$$

的判别式.
由判别式与结式的关系 $\mathrm{Disc}(fg) = \mathrm{Disc}(f)\,\mathrm{Disc}(g)\,\mathrm{Res}(f,g)^2$, 取 $f = x$, $g = x^3 - s_1x^2 + s_2x - s_3$. 有 $\mathrm{Disc}(x) = 1$, $\mathrm{Res}(x, g) = g(0) = -s_3$, 故

$$\Delta(s_1, s_2, s_3, 0) = s_3^2 \cdot \mathrm{Disc}(g).$$

三次多项式 x^3+ax^2+bx+c 的判别式为 $a^2b^2-4b^3-4a^3c-27c^2+18abc$, 代入 $a = -s_1$, $b = s_2$, $c = -s_3$ 得

$$\mathrm{Disc}(g) = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2 + 18s_1s_2s_3.$$

再乘 s_3^2, 得到 Δ 中全部不被 s_4 整除的项:

$$\Delta = s_1^2s_2^2s_3^2 - 4s_2^3s_3^2 - 4s_1^3s_3^3 - 27s_3^4 + 18s_1s_2s_3^3 + (\text{含}s_4\text{ 的项}).$$

即各系数为: $s_1^2s_2^2s_3^2 : 1$, $s_2^3s_3^2 : -4$, $s_1^3s_3^3 : -4$, $s_3^4 : -27$, $s_1s_2s_3^3 : 18$. 其余不被 s_4 整除的单项式 (如 s_1^{12}, $s_1^{10}s_2$ 等) 系数为 0.

习题 7.11

Prove that the only subgroup of order 12 of the symmetric group S_4 is the alternating group A_4.

解答　习题 7.11

题目翻译: 证明对称群 S_4 的唯一的 12 阶子群是交错群 A_4.
解答: 设 $H \le S_4$ 且 $|H| = 12$. 因 $[S_4 : H] = 24/12 = 2$, H 是指标 2 的子群, 故正规: 对 $g \notin H$, 左陪集为 H 与 gH, 右陪集为 H 与 Hg, 而 gH 与 Hg 都等于 H 在 S_4 中的补集, 故 $gH = Hg$, 于是 H 正规.
商群 $S_4/H \cong C_2$ 交换. 自然同态 $S_4 \to S_4/H$ 的核是 H, 而到交换群的同态之核必包含换位子子群, 故 $H \supseteq [S_4, S_4]$. 对称群的换位子子群是交错群, 即 $[S_4, S_4] = A_4$ (例如三循环 $(abc) = (ab)(ac)(ab)(ac) = [(ab), (ac)]$ 都是换位子, 而三循环生成 A_4). 于是 $A_4 \subseteq H$. 又 $|A_4| = 12 = |H|$, 故 $H = A_4$.

习题 8.3

Exhibit the bijective map (6.8.4) explicitly, when G is the dihedral group D_4 and S is the set of vertices of a square.

解答　习题 8.3

题目翻译: 当 G 是二面体群 D_4, S 是正方形的顶点集时, 具体写出双射映射 (6.8.4).
解答: 映射 (6.8.4) 是轨道-稳定子定理中的双射 $\varphi : G/G_x \to Gx$, $gG_x \mapsto g \cdot x$. 取顶点集 $S = \{1, 2, 3, 4\}$ 按顺时针排列, 设 r 是绕中心旋转 90 度 ($r(i) = i + 1 \bmod 4$), s 是关于过顶点 1, 3 的对角线的反射, 则

$$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\},$$

且 s 固定顶点 1. 取 $x = 1$, 稳定子 $G_1 = \{1, s\}$, 它有 4 个左陪集:

左陪集	φ 的像
$G_1 = \{1, s\}$	$1 \cdot 1 = 1$
$rG_1 = \{r, rs\}$	$r(1) = 2$
$r^2G_1 = \{r^2, r^2s\}$	$r^2(1) = 3$
$r^3G_1 = \{r^3, r^3s\}$	$r^3(1) = 4$

其中 rs, r^2s, r^3s 分别作用在 1 上也为 $2, 3, 4$, 与所在陪集一致. 于是 $\varphi : G/G_1 \to \{1, 2, 3, 4\}$, $gG_1 \mapsto g(1)$, 把上述四个陪集分别映到 $1, 2, 3, 4$, 是一个双射, 且与 D_4 的作用相容.

习题 9.2

Let G be the group of rotational symmetries of a cube, let G_v, G_e, G_f be the stabilizers of a vertex v, an edge e, and a face f of the cube, and let V, E, F be the sets of vertices, edges, and faces, respectively. Determine the formulas that represent the decomposition of each of the three sets into orbits for each of the subgroups.

解答　习题 9.2

题目翻译: 设 G 是立方体的旋转群, G_v, G_e, G_f 分别是顶点 v, 棱 e, 面 f 的稳定子, V, E, F 分别是顶点集, 棱集, 面集. 对每个子群, 分别写出 V, E, F 分解为轨道 (轨道长度的分拆) 的公式.
解答:$|G| = 24$, 由轨道-稳定子定理, $|G_v| = 24/8 = 3$, $|G_e| = 24/12 = 2$, $|G_f| = 24/6 = 4$. 每个子群作用在 V, E, F 上, 各轨道长度是该子群阶数的因数.
$G_v \cong C_3$ (绕体对角线 v 与对顶点旋转 120 度).

$$V = 1 + 1 + 3 + 3, \qquad E = 3 + 3 + 3 + 3, \qquad F = 3 + 3.$$

说明: 顶点被固定两个 (v 与对顶点), 其余 6 个顶点分成两个 3 元素轨道; 棱中从 v 出发的 3 条与从对顶点出发的 3 条各成一轨道, 其余 6 条棱分成两个 3 元素轨道; 面中

交于 v 的 3 个与交于对顶点的 3 个各成一轨道.
$G_e \cong C_2$ (绕过 e 与对棱中点的轴旋转 180 度).

$$V = 2+2+2+2, \qquad E = 1+1+2+2+2+2+2, \qquad F = 2+2+2.$$

说明: 顶点中 e 的两个端点交换, 对棱的两个端点交换, 其余 4 个顶点两两交换; 棱中 e 与对棱被固定, 其余 10 条棱两两交换; 6 个面两两交换.
$G_f \cong C_4$ (绕过面心的轴旋转 90 度).

$$V = 4+4, \qquad E = 4+4+4, \qquad F = 1+1+4.$$

说明: 顶点分成上下两个正方形环, 各 4 个; 棱分成上环 4 条, 下环 4 条, 竖直 4 条; 面中 f 与对立面被固定, 4 个侧面成一 4 元素轨道.

习题 9.4

Identify the group T' of all symmetries of a regular tetrahedron, including orientation-reversing symmetries.

解答　习题 9.4

题目翻译: 识别正四面体的全对称群 T' (含反转定向的对称).
解答: 正四面体有 4 个顶点, 其形状由顶点完全确定, 故一个对称由它在顶点上的作用唯一决定, 这给出单同态 $T' \to S_4$, 故 $|T'| \le 24$.
正四面体的旋转群阶数为 12, 同构于 A_4 (旋转群传递地作用在 4 个顶点上, 且每个旋转保持定向, 给出 A_4). 反转定向的对称还能实现奇置换: 例如取过一条棱与该棱的对棱的中点的平面, 关于此平面的反射固定该棱 (及平面), 而交换另外两个顶点, 实现一个对换. 对换生成 S_4, 故 T' 的像为整个 S_4.
因此 $T' \cong S_4$, 阶数为 24. 其中保持定向的 12 个 (偶置换) 由旋转实现, 反转定向的 12 个 (奇置换) 由反射, 旋转反演等实现.

习题 10.1

Determine the orders of the orbits for left multiplication on the set of subsets of order 3 of D_3.

解答　习题 10.1

题目翻译: 求左乘作用在 D_3 的三元子集集合上时各轨道的阶.
解答: $D_3 = \{1, r, r^2, s, sr, sr^2\}$, 其中 $r^3 = s^2 = 1$, $sr = r^2 s$, $|D_3| = 6$. 三元子集共有 $\binom{6}{3} = 20$ 个. 左乘作用 $g \cdot U = gU$ 下, 由轨道-稳定子定理, 轨道长度乘稳定子阶数等于 6, 故轨道长度只可能为 1, 2, 3, 6.

左乘 r 在 D_3 上的循环分解为 $(1\ \ r\ \ r^2)(s\ \ sr\ \ sr^2)$. 一个三元子集被 r 保持当且仅当它是整条循环的并, 即 $U_1=\{1,r,r^2\}$ 或 $U_2=\{s,sr,sr^2\}$. 两者的稳定子为 3 阶子群 $\{1,r,r^2\}$, 轨道长度为 $6/3=2$, 且 $sU_1=\{s,sr,sr^2\}=U_2$, 故 U_1,U_2 构成一个 2 元素轨道.
左乘二阶元素 s,sr,sr^2 的循环分解都由对换组成, 不可能保持三元子集; 故其余 18 个三元子集的稳定子都平凡, 每个轨道长度为 6, 共 $18/6=3$ 个 6 元素轨道.
所以轨道阶数为: 一个长度为 2 的轨道, 三个长度为 6 的轨道.

习题 2.7

Rule out as many as you can, as class equations for a group of order 10:
$1+1+1+2+5$, $1+2+2+5$, $1+2+3+4$, $1+1+2+2+2+2$.

解答　习题 2.7

题目翻译: 对 10 阶群的类方程, 尽可能多地排除下列候选: $1+1+1+2+5$, $1+2+2+5$, $1+2+3+4$, $1+1+2+2+2+2$.
解答: 类方程中每一项都是共轭类大小, 必整除 $|G|=10$, 故只能为 1, 2, 5; 且 1 的个数等于 $|Z(G)|$, 而 $|Z(G)|$ 整除 10.
$1+1+1+2+5$: 有 3 个 1, 故 $|Z(G)|=3$, 但 $3\nmid 10$, 排除.
$1+2+3+4$: 含大小为 3 与 4 的共轭类, 但 $3\nmid 10$ 且 $4\nmid 10$, 排除.
$1+1+2+2+2+2$: $|Z(G)|=2$, 则 $|G/Z(G)|=5$ 为素数, $G/Z(G)$ 循环. 若 $G/Z(G)$ 循环则 G 交换 (此时 $G=Z(G)$), 与 $|Z(G)|=2<10$ 矛盾, 排除.
$1+2+2+5$: 不能排除, 它正是 D_5 的类方程. 事实上 $D_5=\langle a,b:a^5=b^2=1,\ bab^{-1}=a^{-1}\rangle$ 的中心为 $\{1\}$, 共轭类为 $\{1\}$, $\{a,a^4\}$, $\{a^2,a^3\}$, $\{b,ab,a^2b,a^3b,a^4b\}$.
因此四个候选中只有 $1+2+2+5$ 可能, 且确为 D_5 的类方程.

习题 2.9

Determine the class equation for the following groups: (a) the quaternion group, (b) D_4, (c) D_5, (d) the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of invertible upper triangular matrices.

解答　习题 2.9

题目翻译: 求下列群的类方程: (a) 四元数群, (b) D_4, (c) D_5, (d) $\mathrm{GL}_2(\mathbb{F}_3)$ 中可逆上三角矩阵构成的子群.
解答:(a) 四元数群 $Q_8=\{\pm1,\pm i,\pm j,\pm k\}$, 中心 $\{\pm1\}$. 共轭类为 $\{1\}$, $\{-1\}$, $\{i,-i\}$, $\{j,-j\}$, $\{k,-k\}$, 故类方程为 $1+1+2+2+2=8$.
(b) $D_4=\{1,r,r^2,r^3,s,sr,sr^2,sr^3\}$, 中心 $\{1,r^2\}$. 共轭类为 $\{1\}$, $\{r^2\}$, $\{r,r^3\}$, $\{s,sr^2\}$, $\{sr,sr^3\}$, 类方程为 $1+1+2+2+2=8$.
(c) D_5: 共轭类为 $\{1\}$, $\{a,a^4\}$, $\{a^2,a^3\}$, $\{b,ab,a^2b,a^3b,a^4b\}$, 类方程为 $1+2+2+5=10$.
(d) 记 B 为上三角可逆矩阵全体: $B=\{\left[\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right]:a,d\in\mathbb{F}_3^*,\ b\in\mathbb{F}_3\}$, $|B|=2\cdot2\cdot3=12$. 先

求中心: $\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]$ 与 $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ 可交换给出 $a = d$, 与 $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right]$ 可交换给出 $b = 0$, 故 $Z(B) = \{I, 2I\}$, 阶数为 2.
计算共轭: 对 $T = \left[\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right] \in B$,

$$T\left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]T^{-1} = \left[\begin{smallmatrix} a & (xb+y(d-a))z^{-1} \\ 0 & d \end{smallmatrix}\right],$$

其中 $x, z \in \mathbb{F}_3^*$, $y \in \mathbb{F}_3$. 对角元 a, d 不变. 若 $a \neq d$, $y(d-a)$ 跑遍 $\mathbb{F}_3$, 故所有 b 在同一类, 得两个 3 阶共轭类, 对应 $(a, d) = (1, 2), (2, 1)$. 若 $a = d$, b 只能被非零标量乘, 故 $(a, d) = (1, 1)$ 给出 $\{I\}$ (1 阶) 与 $\{\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]\}$ (2 阶); $(a, d) = (2, 2)$ 给出 $\{2I\}$ 与 $\{\left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & 2 \\ 0 & 2 \end{smallmatrix}\right]\}$. 故类方程为

$$1 + 1 + 2 + 2 + 3 + 3 = 12.$$

习题 2.14

The class equation of a group G is $1 + 4 + 5 + 5 + 5$. (a) Does G have a subgroup of order 5? If so, is it a normal subgroup? (b) Does G have a subgroup of order 4? If so, is it a normal subgroup?

解答　习题 2.14

题目翻译: 群 G 的类方程是 $1 + 4 + 5 + 5 + 5$. (a) G 是否有 5 阶子群? 若有, 它是否正规? (b) G 是否有 4 阶子群? 若有, 它是否正规?
解答: $|G| = 1 + 4 + 5 + 5 + 5 = 20$.
(a) 存在. 取共轭类大小为 4 的元素 x, 由轨道-稳定子定理 $|C_G(x)| = 20/4 = 5$, 故 $C_G(x)$ 是 5 阶子群, 记为 H (因 5 为素数, H 循环). 正规性: 5 阶元素 g 满足 $|C_G(g)| \geq 5$ (因 $C_G(g)$ 含 g 且 g 的阶为 5), 故其共轭类大小 $= |G|/|C_G(g)| \leq 4$, 只可能是 1 或 4. 类方程中只有一个 1 (中心平凡), 故所有 5 阶元素正好是那个 4 阶共轭类中的 4 个元素. 任取其一 x, $\langle x\rangle$ 含 1 与这 4 个元素 (因 $\langle x\rangle \setminus \{1\}$ 的元素都是 5 阶元素, 都在那个 4 阶类中), 故 $\{1\} \cup$ (4 阶共轭类) $= \langle x\rangle$ 就是唯一的 5 阶子群 H. 由于 H 是共轭类的并, 它是正规子群.
(b) 存在. 取共轭类大小为 5 的元素 y, 则 $|C_G(y)| = 20/5 = 4$, 故 $C_G(y)$ 是 4 阶子群. 正规性: 设 L 是 G 的任一 4 阶子群. 由 (a), H 是正规 5 阶子群. 因 $\gcd(4, 5) = 1$, $L \cap H = \{1\}$, 故 $|LH| = |L||H|/|L \cap H| = 20 = |G|$, 于是 $G = LH$. 若 L 正规, 则 $G \cong L \times H$ 是交换群, 其类方程应为 $1 + 1 + \cdots + 1$ (20 个 1), 与已知类方程矛盾. 故 L 不正规, 特别地 $C_G(y)$ 不正规.

习题 2.17

Use the class equation to show that a group of order pq, with p and q prime, contains an element of order p.

解答　习题 2.17

题目翻译: 用类方程证明: 阶为 pq (p, q 为素数) 的群含有 p 阶元素.
解答: 若 $p=q$, 则 $|G|=p^2$. 取非平凡元素 g, 其阶整除 p^2 (Lagrange 定理), 故阶为 p 或 p^2; 若阶为 p^2, 则 g^p 的阶为 p. 已得.
下设 $p\neq q$, 不妨 $p>q$, 反设 G 没有 p 阶元素. 则每个非平凡元素的阶都是 q: 元素的阶整除 pq, 若阶为 p 或 pq, 都会给出 p 阶元素 (阶为 pq 时取其 q 次幂).
于是对非中心元素 x, 其共轭类大小 $[G:C_G(x)]$ 整除 pq 且大于 1. 因 $C_G(x)\supseteq\langle x\rangle$ (阶 q), $|C_G(x)|\in\{q,pq\}$; 非中心元素不可能有 $|C_G(x)|=pq$ (否则 $C_G(x)=G$, $x\in Z(G)$), 故 $|C_G(x)|=q$, 共轭类大小为 p. 类方程写为

$$pq=|Z(G)|+p\,m,$$

其中 m 是非中心共轭类个数. 故 $p\mid|Z(G)|$, 又 $|Z(G)|$ 整除 pq, 得 $|Z(G)|\in\{p,pq\}$.
若 $|Z(G)|=p$, 则 $|G/Z(G)|=q$ 为素数, $G/Z(G)$ 循环, 推出 G 交换, 于是 $Z(G)=G$, 与 $|Z(G)|=p<pq$ 矛盾. 故 $|Z(G)|=pq$, 即 G 交换. 取非平凡元素 a (阶为 q), $\langle a\rangle\trianglelefteq G$ (G 交换). 商群 $G/\langle a\rangle$ 的阶数为 $pq/q=p$, 其非平凡元素阶为 p; 但它是某个 $g\langle a\rangle$, 而 g 的阶整除 q, 故 $g\langle a\rangle$ 的阶也整除 q, 矛盾.
所以反设不成立, G 含有 p 阶元素.

习题 1.3

Let $w_k=u_1^k+\cdots+u_n^k$. (a) Prove Newton's identities: $w_k-s_1w_{k-1}+\cdots\pm s_{k-1}w_1\mp ks_k=0$. (b) Do $w_1,\ldots,w_n$ generate the ring of symmetric functions?

解答　习题 1.3

题目翻译: 设 $w_k=u_1^k+\cdots+u_n^k$. (a) 证明 Newton 恒等式: $w_k-s_1w_{k-1}+\cdots\pm s_{k-1}w_1\mp ks_k=0$. (b) $w_1,\ldots,w_n$ 是否生成对称函数环?
解答:(a) 记 $s_0=1$, 约定 $j>n$ 时 $s_j=0$. 考虑多项式 $P(t)=\prod_{i=1}^n(1-u_it)=\sum_{j=0}^n(-1)^js_jt^j$. 对数导数给出

$$\frac{P'(t)}{P(t)}=\sum_{i=1}^n\frac{-u_i}{1-u_it}=-\sum_{i=1}^n u_i\sum_{m\geq0}u_i^mt^m=-\sum_{m\geq0}w_{m+1}t^m,$$

故 $P'(t)=-P(t)\sum_{m\geq0}w_{m+1}t^m$. 比较两边 t^{k-1} 的系数 ($k\geq1$): 左边为 $(-1)^kks_k$, 右边为 $-\sum_{j=0}^{k-1}(-1)^js_jw_{k-j}$. 于是

$$(-1)^kks_k=-\sum_{j=0}^{k-1}(-1)^js_jw_{k-j},\qquad\sum_{j=0}^{k-1}(-1)^js_jw_{k-j}+(-1)^kks_k=0,$$

即

$$w_k-s_1w_{k-1}+s_2w_{k-2}-\cdots+(-1)^{k-1}s_{k-1}w_1+(-1)^kks_k=0.$$

这就是 Newton 恒等式 (对 $k \le n$; $k > n$ 时只需令 $s_k = 0$, 公式仍成立).
(b) 在有理数域 (或任何特征 0 的域) 上, 生成. 由 (a) 可递归地把 s_k 表示成 $w_1, \dots, w_k$ 的多项式:

$$s_k = \frac{(-1)^{k+1}}{k}\Big(w_k - s_1 w_{k-1} + s_2 w_{k-2} - \cdots + (-1)^{k-1} s_{k-1} w_1\Big).$$

初等对称函数 $s_1, \dots, s_n$ 生成对称函数环 (对称函数基本定理), 而每个 s_k 又是 $w_1, \dots, w_n$ 的多项式, 故 $w_1, \dots, w_n$ 生成对称函数环.
在整数环 $\mathbb{Z}$ 上则不生成: 例如 $w_2 = s_1^2 - 2s_2$ 给出 $s_2 = (w_1^2 - w_2)/2$, 而 2 在 $\mathbb{Z}$ 中不可逆, $(w_1^2 - w_2)/2$ 不是整系数多项式.

6

第六次作业

习题 5.1

For each of the following sets of automorphisms of the field of rational functions $\mathbb{C}(t)$, determine the group of automorphisms that they generate, and determine the fixed field explicitly.
(a) $\sigma(t) = t^{-1}$,
(b) $\sigma(t) = \mathrm{i}t$,
(c) $\sigma(t) = -t$,
(d) $\sigma(t) = \omega t$, where $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$,
(e) $\tau(t) = t^{-1}$.

解答

题目翻译: 对有理函数域 $\mathbb{C}(t)$ 的下列各组自同构, 求出它们生成的自同构群, 并显式求出该群的不动域.
解答: 记 $\langle\sigma\rangle$ 为自同构 σ 生成的群. 由 Artin 定理 (有限自同构群 G 在域 E 上的不动域满足 $[E : E^G] = |G|$), 阶为 n 的自同构 σ 满足 $[\mathbb{C}(t) : \mathbb{C}(t)^{\langle\sigma\rangle}] = n$. 于是只要找到一个 $u \in \mathbb{C}(t)^{\langle\sigma\rangle}$ 使 $[\mathbb{C}(t) : \mathbb{C}(u)] = n$, 不动域就是 $\mathbb{C}(u)$.
(a) $\sigma(t) = t^{-1}$, 则 $\sigma^2(t) = t$, 故 $\langle\sigma\rangle = \{1, \sigma\} \cong \mathbb{Z}/2$. 取 $u = t + t^{-1}$, 则 $\sigma(u) = \sigma(t) + \sigma(t)^{-1} = t^{-1} + t = u$, 故 u 被 σ 固定. 又 t 满足二次方程 $T^2 - uT + 1 = 0$; 若 $t \in \mathbb{C}(u)$, 则 σ 固定 $\mathbb{C}(u) = \mathbb{C}(t)$, 推出 $\sigma = 1$, 矛盾, 故 $[\mathbb{C}(t) : \mathbb{C}(u)] = 2$. 因此不动域为 $\mathbb{C}(t + t^{-1})$.

(b) $\sigma(t)=\mathrm{i}t$, 则 $\sigma^2(t)=-t$, $\sigma^3(t)=-\mathrm{i}t$, $\sigma^4(t)=t$, 故 $\langle\sigma\rangle\cong\mathbb{Z}/4$. 取 $u=t^4$, 则 $\sigma(u)=(\mathrm{i}t)^4=t^4=u$. 多项式 T^4-u 在 $\mathbb{C}(u)$ 上不可约 (在 $\mathbb{C}[u]$ 中取素元 u 用 Eisenstein 判别法), 故 $[\mathbb{C}(t):\mathbb{C}(t^4)]=4$. 不动域为 $\mathbb{C}(t^4)$.
(c) $\sigma(t)=-t$, $\sigma^2(t)=t$, 故 $\langle\sigma\rangle\cong\mathbb{Z}/2$. 取 $u=t^2$, 则 $\sigma(u)=t^2=u$, 且 T^2-u 不可约, $[\mathbb{C}(t):\mathbb{C}(t^2)]=2$. 不动域为 $\mathbb{C}(t^2)$.
(d) $\sigma(t)=\omega t$, $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$, 则 $\sigma^2(t)=\omega^2t$, $\sigma^3(t)=\omega^3t=t$, 故 $\langle\sigma\rangle\cong\mathbb{Z}/3$. 取 $u=t^3$, 则 $\sigma(u)=(\omega t)^3=t^3=u$, 且 T^3-u 不可约, $[\mathbb{C}(t):\mathbb{C}(t^3)]=3$. 不动域为 $\mathbb{C}(t^3)$.
(e) $\tau(t)=t^{-1}$ 与 (a) 相同: $\langle\tau\rangle=\{1,\tau\}\cong\mathbb{Z}/2$, 不动域为 $\mathbb{C}(t+t^{-1})$.

习题 6.2

Let $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Determine $[K:\mathbb{Q}]$, prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

解答

题目翻译: 设 $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. 求 $[K:\mathbb{Q}]$, 证明 K 是 $\mathbb{Q}$ 的 Galois 扩张, 并确定其 Galois 群.
解答: 次数. $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ (x^2-2 不可约). 若 $\sqrt{3}=a+b\sqrt{2}$ ($a,b\in\mathbb{Q}$), 平方后比较 $\{1,\sqrt{2}\}$ 的系数得 $2ab=0$ 且 $a^2+2b^2=3$, 无解, 故 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, 于是 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$, 且 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 在 $\mathbb{Q}$ 上的基.
再证 $\sqrt{5}\notin\mathbb{Q}(\sqrt{2},\sqrt{3})$. 反设 $\sqrt{5}=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ ($a,b,c,d\in\mathbb{Q}$), 两边平方并比较基 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 的系数, 得

$$a^2+2b^2+3c^2+6d^2=5,\qquad ab+3cd=0,\qquad ac+2bd=0,\qquad ad+bc=0.$$

由 $ab+3cd=0$, $ac+2bd=0$, $ad+bc=0$ 消元可得 $d(a^2-2b^2)=0$ 与 $b(a^2-3c^2)=0$. 若 $a\neq0$: 当 $d\neq0$ 时 $a^2=2b^2$ 迫使 $(a/b)^2=2\notin\mathbb{Q}$, 矛盾; 当 $d=0$ 时由 $ad+bc=0$ 与 $ac+2bd=0$ 得 $c=0$, 再由 $ab+3cd=0$ 得 $b=0$, 于是 $\sqrt{5}=a\in\mathbb{Q}$, 矛盾. 若 $a=0$, 则 $bc=bd=cd=0$, 即 b,c,d 至多一个非零, 但 $\sqrt{5}$ 不可能等于某有理数乘 $\sqrt{2}$, $\sqrt{3}$ 或 $\sqrt{6}$ (平方后 $5=2b^2$, $3c^2$ 或 $6d^2$ 均无有理数解). 因此 $\sqrt{5}\notin\mathbb{Q}(\sqrt{2},\sqrt{3})$, 从而 $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})]=2$. 故

$$[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})]\,[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=2\cdot4=8.$$

Galois 性. K 是多项式 $f(x)=(x^2-2)(x^2-3)(x^2-5)\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域 (其全部根 $\pm\sqrt{2},\pm\sqrt{3},\pm\sqrt{5}$ 生成 K). 特征 0 的多项式可分, 而有限 Galois 扩张等价于可分多项式的分裂域, 故 $K/\mathbb{Q}$ 是 Galois 扩张.
Galois 群. 因 $K/\mathbb{Q}$ 是分裂域, 其每个 $\mathbb{Q}$-自同构由根上的置换决定. 由于 $\sqrt{2},\sqrt{3},\sqrt{5}$ 的极小多项式分别为 x^2-2,x^2-3,x^2-5, 每个自同构必须把 $\sqrt{2}$ 映到 $\pm\sqrt{2}$, $\sqrt{3}$ 映到 $\pm\sqrt{3}$, $\sqrt{5}$ 映到 $\pm\sqrt{5}$. 反过来, 这 $2^3=8$ 种独立符号选择都定义 $\mathbb{Q}$-

同构 (对基 $\{1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{10},\sqrt{15},\sqrt{30}\}$ 上系数作相应变号即保持运算), 而 $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}]=8$ 说明嵌入总数恰为 8, 故这就是全部嵌入; 因 $K/\mathbb{Q}$ 正规, 每个嵌入都是自同构. 因此

$$\mathrm{Gal}(K/\mathbb{Q})\cong\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2=(\mathbb{Z}/2)^3.$$

习题 7.3

How many intermediate fields L with $[L:F]=2$ are there when K/F is a Galois extension with Galois group (a) the alternating group A_4, (b) the dihedral group D_4?

解答

题目翻译: 设 K/F 是 Galois 扩张, 其 Galois 群分别为 (a) 交错群 A_4, (b) 二面体群 D_4. 满足 $[L:F]=2$ 的中间域 L 各有多少个?

解答: 由 Galois 基本定理 (中间域与 Galois 群子群一一对应, 且 $[L:F]=[G:\mathrm{Gal}(K/L)]$), 满足 $[L:F]=2$ 的中间域 L 一一对应于 G 的指数为 2 的子群 $H=\mathrm{Gal}(K/L)$. 指数为 2 的子群必为正规子群.

(a) $G=A_4$, $|A_4|=12$, 指数 2 的子群阶为 6. A_4 的正规子群只有 $\{e\}$, $V_4=\{(1),(12)(34),(13)(24),(14)(23)\}$ 和 A_4 本身, 阶分别为 $1,4,12$, 没有阶为 6 的正规子群. 故 A_4 无指数 2 的子群, 满足 $[L:F]=2$ 的中间域个数为 0.

(b) $G=D_4=\langle r,s\mid r^4=s^2=1,\ srs=r^{-1}\rangle$, $|D_4|=8$, 指数 2 的子群阶为 4. D_4 的阶 4 子群共有 3 个:

$$\langle r\rangle=\{1,r,r^2,r^3\},\qquad \{1,r^2,s,sr^2\},\qquad \{1,r^2,sr,sr^3\}.$$

故满足 $[L:F]=2$ 的中间域个数为 3.

习题 7.6

Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is K the splitting field of an irreducible cubic polynomial over F?

解答

题目翻译: 设 K/F 是 Galois 扩张, 其 Galois 群为对称群 S_3. 问 K 是不是 F 上某个不可约三次多项式的分裂域?

解答: 是.

取一个换位 $\tau\in S_3$, 令 $H=\langle\tau\rangle$, 则 $|H|=2$. 设 $L=\mathrm{Inv}(H)$ 为 H 的不动域. 由 Galois 基本定理, L 是中间域且 $[L:F]=[G:H]=3$. 因为 K/F 是 Galois 扩张故可分, 其子扩张 L/F 也是有限可分扩张, 由本原元定理 $L=F(\beta)$ 对某 $\beta\in L$. 于是 β 在 G 中

的稳定子为

$$\{\sigma \in G : \sigma(\beta) = \beta\} = \mathrm{Gal}(K/F(\beta)) = \mathrm{Gal}(K/L) = H,$$

故 β 的轨道 $\{\sigma(\beta) : \sigma \in G\}$ 恰有 $[G : H] = 3$ 个元素.
令 $m_\beta(x)$ 为 β 在 F 上的极小多项式. 因 K/F 正规, m_β 在 K 中分裂, 且其根恰为轨道中 3 个互异元素, 故 $\deg m_\beta = 3$, 即 m_β 是 F 上的不可约三次多项式. 设 $E \subseteq K$ 为 m_β 在 F 上的分裂域. $G = S_3$ 在 m_β 的三个根上的作用: 换位子群 H 在 S_3 中全体共轭之交为 $\{e\}$, 故该作用忠实, 即 G 同构地作用为 S_3 本身, 于是 $|\mathrm{Gal}(E/F)| = 6 = [K : F]$. 又 $E \subseteq K$, 故 $E = K$. 所以 K 是 F 上不可约三次多项式 m_β 的分裂域.

习题 7.7

(a) Determine the irreducible polynomial for $\mathrm{i} + \sqrt{2}$ over $\mathbb{Q}$. (b) Prove that the set $\{1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2}\}$ is a basis for $\mathbb{Q}(\mathrm{i}, \sqrt{2})$ over $\mathbb{Q}$.

解答

题目翻译:(a) 求 $\mathrm{i} + \sqrt{2}$ 在 $\mathbb{Q}$ 上的不可约多项式. (b) 证明 $\{1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2}\}$ 是 $\mathbb{Q}(\mathrm{i}, \sqrt{2})$ 在 $\mathbb{Q}$ 上的基.
解答: (a) 设 $\gamma = \mathrm{i} + \sqrt{2}$. 由 $\gamma - \sqrt{2} = \mathrm{i}$ 平方得 $(\gamma - \sqrt{2})^2 = -1$, 即 $\gamma^2 - 2\sqrt{2}\gamma + 2 = -1$, 亦即 $\gamma^2 + 3 = 2\sqrt{2}\gamma$. 再平方得 $(\gamma^2+3)^2 = 8\gamma^2$, 即 $\gamma^4 - 2\gamma^2 + 9 = 0$. 故 $f(x) = x^4 - 2x^2 + 9$ 以 γ 为根.
f 的根: 令 $y = x^2$, 则 $y^2 - 2y + 9 = 0$, 解得 $y = 1 \pm 2\sqrt{2}\mathrm{i} = (\sqrt{2} \pm \mathrm{i})^2$, 故 $x = \pm(\sqrt{2} \pm \mathrm{i})$, 即 $\pm\sqrt{2} \pm \mathrm{i}$.
由 $\gamma^2 + 3 = 2\sqrt{2}\gamma$ 得 $\sqrt{2} = (\gamma^2 + 3)/(2\gamma) \in \mathbb{Q}(\gamma)$, 于是 $\mathrm{i} = \gamma - \sqrt{2} \in \mathbb{Q}(\gamma)$, 故 $\mathbb{Q}(\gamma) = \mathbb{Q}(\mathrm{i}, \sqrt{2})$. 而 $[\mathbb{Q}(\mathrm{i}, \sqrt{2}) : \mathbb{Q}] = 4$ (因为 $\mathrm{i} \notin \mathbb{Q}(\sqrt{2})$, 后者为实数域), 所以 $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$, 即 f 是 γ 的极小多项式, 不可约. 故 $\mathrm{i} + \sqrt{2}$ 在 $\mathbb{Q}$ 上的不可约多项式为 $f(x) = x^4 - 2x^2 + 9$, 其根为 $\sqrt{2} + \mathrm{i}$, $\sqrt{2} - \mathrm{i}$, $-\sqrt{2} + \mathrm{i}$, $-\sqrt{2} - \mathrm{i}$.
(b) $[\mathbb{Q}(\mathrm{i}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\mathrm{i}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$. 设 $a + b\mathrm{i} + c\sqrt{2} + d\mathrm{i}\sqrt{2} = 0$ $(a, b, c, d \in \mathbb{Q})$, 写成 $(a + c\sqrt{2}) + (b + d\sqrt{2})\mathrm{i} = 0$. 因 $\{1, \mathrm{i}\}$ 是 $\mathbb{Q}(\mathrm{i}, \sqrt{2})$ 在 $\mathbb{Q}(\sqrt{2})$ 上的基, 得 $a + c\sqrt{2} = 0$, $b + d\sqrt{2} = 0$; 又 $\{1, \sqrt{2}\}$ 是 $\mathbb{Q}(\sqrt{2})$ 在 $\mathbb{Q}$ 上的基, 得 $a = c = 0$, $b = d = 0$. 故这四个元素在 $\mathbb{Q}$ 上线性无关, 个数等于维数 4, 从而是基.

习题 7.10

Let K/F be a Galois extension with Galois group G, and let H be a subgroup of G. Prove that there exists an element $\beta \in K$ whose stabilizer is equal to H.

解答

题目翻译: 设 K/F 是 Galois 扩张, Galois 群为 G, H 是 G 的一个子群. 证明存在 $\beta \in K$ 使 β 的稳定子恰为 H.

解答: 设 $L = \mathrm{Inv}(H)$ 为 H 在 K 中的不动域. 由 Galois 基本定理, L 是中间域且 $\mathrm{Gal}(K/L) = H$.

因为 K/F 是 Galois 扩张, 从而是有限可分扩张, 其子扩张 L/F 也是有限可分扩张. 由本原元定理, 存在 $\beta \in L$ 使 $L = F(\beta)$.

β 在 G 中的稳定子为 $\{\sigma \in G : \sigma(\beta) = \beta\} = \mathrm{Gal}(K/F(\beta))$. 由于 $F(\beta) = L$, 该群等于 $\mathrm{Gal}(K/L) = H$. 故存在 $\beta \in K$ 其稳定子恰为 H, 得证.

习题 8.2

Determine the Galois groups of the following polynomials over $\mathbb{Q}$:

(a) $x^3 - 2$,

(b) $x^3 + 3x + 14$,

(c) $x^3 - 3x^2 + 1$,

(d) $x^3 - 21x + 7$,

(e) $x^3 + x^2 - 2x - 1$,

(f) $x^3 + x^2 - 2x + 1$.

解答

题目翻译: 求下列多项式在 $\mathbb{Q}$ 上的 Galois 群: (a) x^3-2, (b) $x^3+3x+14$, (c) x^3-3x^2+1, (d) $x^3 - 21x + 7$, (e) $x^3 + x^2 - 2x - 1$, (f) $x^3 + x^2 - 2x + 1$.

解答: 方法. 设 $f \in \mathbb{Q}[x]$ 为不可约三次多项式, 则其分裂域的 Galois 群是 S_3 的传递子群, 故只能是 S_3 或 $A_3 \cong \mathbb{Z}/3$; 当且仅当判别式是 $\mathbb{Q}$ 中平方时为 A_3. 原因是 $\sqrt{\Delta} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ 被偶置换固定, 被奇置换变为 $-\sqrt{\Delta}$, 故 $G \subseteq A_3$ 当且仅当 $\sqrt{\Delta} \in \mathbb{Q}$. 对 $x^3 + px + q$, 判别式 $\Delta = -4p^3 - 27q^2$; 对 $x^3 + ax^2 + bx + c$, $\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$. 若三次多项式可约, 其分裂域的 Galois 群即其不可约因式所对应者.

(a) $x^3 - 2$: 由 Eisenstein 判别法 (素数 2) 不可约. $p = 0, q = -2$, $\Delta = -4 \cdot 0 - 27 \cdot 4 = -108$, 非有理数平方. Galois 群为 S_3.

(b) $x^3+3x+14$: 有有理根 -2 (因 $(-2)^3+3(-2)+14 = 0$), 分解为 $(x+2)(x^2-2x+7)$. 二次因式 $x^2 - 2x + 7$ 的判别式为 $4 - 28 = -24$ 非平方, 在 $\mathbb{Q}$ 上不可约, 其分裂域为 $\mathbb{Q}(\sqrt{-6})$, Galois 群为 $\mathbb{Z}/2$. 故原多项式的 Galois 群为 $\mathbb{Z}/2$.

(c) $x^3 - 3x^2 + 1$: 无有理根 (± 1 代入均非零), 不可约. $a = -3, b = 0, c = 1$, $\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc = 0 - 0 + 108 - 27 + 0 = 81 = 9^2$ 是平方. Galois 群为 $A_3 \cong \mathbb{Z}/3$.

(d) $x^3 - 21x + 7$: 无有理根 ($\pm 1, \pm 7$ 代入均非零), 不可约. $p = -21, q = 7$, $\Delta = -4(-21)^3 - 27 \cdot 7^2 = 37044 - 1323 = 35721 = 189^2$ 是平方. Galois 群为 A_3.

(e) x^3+x^2-2x-1: 无有理根, 不可约. $a=1,b=-2,c=-1$, $\Delta=1\cdot 4-4(-8)-4\cdot 1\cdot(-1)-27\cdot 1+18\cdot 1\cdot(-2)\cdot(-1)=4+32+4-27+36=49=7^2$ 是平方. Galois 群为 A_3.
(f) x^3+x^2-2x+1: 无有理根, 不可约. $a=1,b=-2,c=1$, $\Delta=1\cdot 4-4(-8)-4\cdot 1\cdot 1-27\cdot 1+18\cdot 1\cdot(-2)\cdot 1=4+32-4-27-36=-31$, 非平方. Galois 群为 S_3.

习题 5.2

Show that the automorphisms $\sigma(t)=(t+\mathrm{i})/(t-\mathrm{i})$ and $\tau(t)=(\mathrm{i}t-\mathrm{i})/(t+1)$ of $\mathbb{C}(t)$ generate a group isomorphic to the alternating group A_4, and determine the fixed field of this group.

解答

题目翻译: 证明 $\mathbb{C}(t)$ 的自同构 $\sigma(t)=(t+\mathrm{i})/(t-\mathrm{i})$ 与 $\tau(t)=(\mathrm{i}t-\mathrm{i})/(t+1)$ 生成的群同构于交错群 A_4, 并求出该群的不动域.
解答: 阶的计算. 先算各自同构的阶:

$$\sigma^2(t)=\sigma\Big(\frac{t+\mathrm{i}}{t-\mathrm{i}}\Big)=\frac{\frac{t+\mathrm{i}}{t-\mathrm{i}}+\mathrm{i}}{\frac{t+\mathrm{i}}{t-\mathrm{i}}-\mathrm{i}}=\frac{(1+\mathrm{i})(t+1)}{(1-\mathrm{i})(t-1)}=\mathrm{i}\,\frac{t+1}{t-1},\qquad \sigma^3(t)=t.$$

故 σ 的阶为 3. 同理可验 $\tau^3=1$, 且 τ 的阶为 3. 又

$$(\sigma\tau)(t)=\sigma\Big(\frac{\mathrm{i}t-\mathrm{i}}{t+1}\Big)=\frac{(\mathrm{i}t-\mathrm{i})+\mathrm{i}(t+1)}{(\mathrm{i}t-\mathrm{i})-\mathrm{i}(t+1)}=\frac{2\mathrm{i}t}{-2\mathrm{i}}=-t,$$

故 $\sigma\tau$ 的阶为 2. 于是 σ,τ 满足 $a^3=b^3=(ab)^2=1$.
由该表示定义的群即 $(3,3,2)$ 三角群, 也就是四面体的旋转群 A_4, 阶为 12: 事实上 $A_4=\langle(123),(124)\rangle$, 且 $((123)(124))^2=1$, 反之关系 $a^3=b^3=(ab)^2=1$ 恰好给出 A_4 的表示. 因为 $\sigma,\tau,\sigma\tau$ 的阶分别为 $3,3,2$, 商掉 A_4 的唯一非平凡正规子群 V_4 会得到阶 3 的群, 其中无阶 2 元素, 与 $\sigma\tau$ 阶为 2 矛盾, 故 $\langle\sigma,\tau\rangle\cong A_4$, 阶为 12.
不动域. 注意到 $-t=\sigma\tau\in G$. 又因为 $\sigma^{-1}=\sigma^2$ 且 $\sigma^2(t)=\mathrm{i}(t+1)/(t-1)$, 直接计算得

$$\sigma(\sigma\tau)\sigma^{-1}(t)=\sigma\Big(-\mathrm{i}\frac{t+1}{t-1}\Big)=\frac{\mathrm{i}\frac{t+1}{1-t}+\mathrm{i}}{\mathrm{i}\frac{t+1}{1-t}-\mathrm{i}}=\frac{1}{t},$$

故 $1/t\in G$. 因此 $V=\{1,-t,1/t,-1/t\}$ 是 G 的子群, 同构于 Klein 四元群 V_4, 且 $V\triangleleft G$ (V_4 是 A_4 的唯一 2 阶正规子群).
V 的不动域: 取 $w=t^2+t^{-2}$, 则 w 被 $-t$ 与 $1/t$ 固定, 且作为 t 的有理函数次数为 4, 故 $[\mathbb{C}(t):\mathbb{C}(w)]=4$; 由 Artin 定理 $[\mathbb{C}(t):\mathbb{C}(t)^V]=|V|=4$, 得 $\mathbb{C}(t)^V=\mathbb{C}(w)$.
由于 $|G|=12$, $|V|=4$, $V\triangleleft G$, 有 $G/V\cong\mathbb{Z}/3$; σ 的阶为 3 且 $\sigma\notin V$, 故 σ 在 G/V 中

的像生成 G/V. 于是不动域满足

$$\mathbb{C}(t)^G = \left(\mathbb{C}(t)^V\right)^{\langle\sigma\rangle} = \mathbb{C}(w)^{\langle\sigma\rangle}.$$

记 $p = t^2$, 则 $w = p + p^{-1}$. 计算

$$\sigma(w) = \sigma(t)^2 + \sigma(t)^{-2} = 2\frac{p^2 - 6p + 1}{(p+1)^2}, \qquad \sigma^2(w) = \sigma^2(t)^2 + \sigma^2(t)^{-2} = -2\frac{p^2 + 6p + 1}{(p-1)^2}.$$

考虑轨道和 $v = w + \sigma(w) + \sigma^2(w)$. 通分得

$$v = \frac{p^6 - 33p^4 - 33p^2 + 1}{p(p^2-1)^2} = \frac{w^3 - 36w}{w^2 - 4},$$

其中最后一步除以 p^3 并利用 $p^3 + p^{-3} = w^3 - 3w$, $p + p^{-1} = w$. 由构造, v 被 σ 与 V 固定, 故 $v \in \mathbb{C}(t)^G$; 且 v 作为 w 的有理函数次数为 3, 故 $[\mathbb{C}(w) : \mathbb{C}(v)] = 3$. 由 Artin 定理 $[\mathbb{C}(w) : \mathbb{C}(w)^{\langle\sigma\rangle}] = 3$, 故 $\mathbb{C}(w)^{\langle\sigma\rangle} = \mathbb{C}(v)$.
于是 G 的不动域为

$$\mathbb{C}(t)^G = \mathbb{C}\left(\frac{w^3 - 36w}{w^2 - 4}\right), \qquad w = t^2 + t^{-2}.$$

习题 6.3

Let $K \supset L \supset F$ be a chain of extension fields of degree 2. Show that K can be generated over F by the root of an irreducible quartic polynomial of the form $x^4 + bx^2 + c$.

解答

题目翻译: 设 $K \supset L \supset F$ 是一列二次扩张, 即 $[K : L] = [L : F] = 2$. 证明 K 可由 F 上某个形如 $x^4 + bx^2 + c$ 的不可约四次多项式的根生成.
解答: 因为 $[L : F] = 2$, 存在非平方元 $a \in F$ 使 $L = F(\sqrt{a})$. 因为 $[K : L] = 2$, 存在 $d \in L$ (非 L 中平方) 使 $K = L(\alpha)$, $\alpha^2 = d$. 把 d 写成 $d = u + v\sqrt{a}$ $(u, v \in F)$.
情形 1: $v \neq 0$. 取 $\gamma = \alpha$. 则 $\gamma^2 = d = u + v\sqrt{a}$, 且 $F(d) = F(u + v\sqrt{a}) = F(\sqrt{a}) = L$. 故 $F(\gamma) \supseteq F(\gamma^2) = L$; 又 $\gamma \notin L$ ($[K : L] = 2$), 故 $[F(\gamma) : L] = 2$, 从而 $[F(\gamma) : F] = [F(\gamma) : L] \cdot [L : F] = 4$. 因 $F(\gamma) \subseteq K$ 且 $[K : F] = 4$, 得 $F(\gamma) = K$. 验证

$$\gamma^4 - 2u\gamma^2 + (u^2 - v^2 a) = (u + v\sqrt{a})^2 - 2u(u + v\sqrt{a}) + u^2 - v^2 a = 0,$$

故 γ 是 $x^4 - 2ux^2 + (u^2 - v^2 a)$ 的根, 该多项式形如 $x^4 + bx^2 + c$ (取 $b = -2u$, $c = u^2 - v^2 a$), 且因 $[F(\gamma) : F] = 4$ 而不可约.
情形 2: $v = 0$. 则 $d = u \in F$, $K = F(\sqrt{a}, \sqrt{u})$, 且 $\sqrt{u} \notin F(\sqrt{a})$ (否则 $[K : F] = 2$).

取 $\gamma=\sqrt{a}+\sqrt{u}$. 则

$$\gamma^2=a+u+2\sqrt{au},\qquad \Big(\gamma^2-(a+u)\Big)^2=4au,$$

即 γ 满足 $x^4-2(a+u)x^2+(a-u)^2=0$, 形如 x^4+bx^2+c (取 $b=-2(a+u)$, $c=(a-u)^2$).
还需证明该多项式不可约且 γ 生成 K. $K=F(\sqrt{a},\sqrt{u})$ 是 $(x^2-a)(x^2-u)$ 在 F 上的分裂域, 为 Galois 扩张, Galois 群为 V_4 (两个符号变化), 其含 F 的子域只有 K, F 与三个二次中间域 $F(\sqrt{a})$, $F(\sqrt{u})$, $F(\sqrt{au})$. 若 $\gamma\in F(\sqrt{a})$, 则 $\sqrt{u}=\gamma-\sqrt{a}\in F(\sqrt{a})$, 矛盾; 同理 $\gamma\notin F(\sqrt{u})$; 若 $\gamma\in F(\sqrt{au})$, 在基 $\{1,\sqrt{a},\sqrt{u},\sqrt{au}\}$ 下比较系数立即矛盾. 故 γ 不属于任何真子域, $[F(\gamma):F]=4$, 从而 $F(\gamma)=K$, 且上述四次多项式不可约. 两种情形均完成证明.

习题 7.5

Let $f(x)$ be an irreducible cubic polynomial over $\mathbb{Q}$ whose Galois group is S_3. Determine the possible Galois groups of the polynomial $(x^3-1)f(x)$.

解答

题目翻译: 设 $f(x)$ 是 $\mathbb{Q}$ 上 Galois 群为 S_3 的不可约三次多项式. 求多项式 $(x^3-1)f(x)$ 在 $\mathbb{Q}$ 上可能的 Galois 群.
解答: 设 K 为 f 在 $\mathbb{Q}$ 上的分裂域, 则 $\mathrm{Gal}(K/\mathbb{Q})\cong S_3$, $[K:\mathbb{Q}]=6$. 又 $x^3-1=(x-1)(x^2+x+1)$, 其分裂域为分圆域 $\mathbb{Q}(\omega)$, $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$ 为本原 3 次单位根, 且 $[\mathbb{Q}(\omega):\mathbb{Q}]=\varphi(3)=2$ (分圆多项式 x^2+x+1 的次数), $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\cong\mathbb{Z}/2$. 设 M 为 $g(x)=(x^3-1)f(x)$ 在 $\mathbb{Q}$ 上的分裂域, 则 $M=K\cdot\mathbb{Q}(\omega)$.
由 Galois 基本定理, S_3 的指数 2 子群唯一 (即 A_3), 故 K 有唯一的二次子域, 即 f 的判别式 D 决定的 $\mathbb{Q}(\sqrt{D})$. 而 $\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{-3})$. 分两种情形:
(1) 若 $D/(-3)$ 是 $\mathbb{Q}$ 中的平方 (即 $\sqrt{-3}\in K$, 等价于 $\mathbb{Q}(\omega)\subseteq K$), 则 $M=K$, 故 $\mathrm{Gal}(M/\mathbb{Q})\cong S_3$.
(2) 若 $D/(-3)$ 不是平方, 则 $K\cap\mathbb{Q}(\omega)=\mathbb{Q}$. 两个 Galois 扩张 $K/\mathbb{Q}$ 与 $\mathbb{Q}(\omega)/\mathbb{Q}$ 的交为 $\mathbb{Q}$ 时, 复合域的 Galois 群同构于两者的直积 (标准事实), 故 $\mathrm{Gal}(M/\mathbb{Q})\cong S_3\times\mathbb{Z}/2$, 阶为 12.
因此 $(x^3-1)f(x)$ 在 $\mathbb{Q}$ 上的 Galois 群只可能是 S_3 或 $S_3\times\mathbb{Z}/2$. 两种都可能出现: 如 $f(x)=x^3-2$ 的判别式 $D=-108=-3\cdot6^2$, 此时 $\mathbb{Q}(\omega)\subseteq K$, 得 S_3; 如 $f(x)=x^3+x+1$ 的判别式 $D=-31$, 得 $S_3\times\mathbb{Z}/2$.

习题 7.11

Let $\alpha=\sqrt[3]{2}$, $\beta=\sqrt{3}$, $\gamma=\alpha+\beta$. Let $L=\mathbb{Q}(\alpha,\beta)$, and let K be the splitting field of the polynomial $(x^3-2)(x^2-3)$ over $\mathbb{Q}$. (a) Determine the irreducible polynomial f for

γ over $\mathbb{Q}$, and its roots in $\mathbb{C}$. (b) Determine the Galois group of $K/\mathbb{Q}$.

解答

题目翻译: 设 $\alpha=\sqrt[3]{2}$, $\beta=\sqrt{3}$, $\gamma=\alpha+\beta$, $L=\mathbb{Q}(\alpha,\beta)$, K 为 $(x^3-2)(x^2-3)$ 在 $\mathbb{Q}$ 上的分裂域. (a) 求 γ 在 $\mathbb{Q}$ 上的不可约多项式 f 及其在 $\mathbb{C}$ 中的根. (b) 求 $K/\mathbb{Q}$ 的 Galois 群.

解答: (a) 由 $\gamma=\alpha+\beta$ 得 $\gamma-\beta=\alpha$, 两边立方: $(\gamma-\beta)^3=\alpha^3=2$, 展开得

$$\gamma^3-3\gamma^2\beta+3\gamma\beta^2-\beta^3=2.$$

因 $\beta^2=3$, $\beta^3=3\beta$, 整理为 $\gamma^3+9\gamma-2=3\beta(\gamma^2+1)$. 平方得 $(\gamma^3+9\gamma-2)^2=27(\gamma^2+1)^2$, 展开得 $\gamma^6-9\gamma^4-4\gamma^3+27\gamma^2-36\gamma-23=0$. 故取

$$f(x)=x^6-9x^4-4x^3+27x^2-36x-23.$$

不可约性: x^3-2 由 Eisenstein 判别法不可约, 故 $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. 又 $\mathbb{Q}(\alpha)\subset\mathbb{R}$, 且若 $\sqrt{3}\in\mathbb{Q}(\alpha)$ 则 $[\mathbb{Q}(\alpha):\mathbb{Q}]$ 被 2 整除, 矛盾, 故 x^2-3 在 $\mathbb{Q}(\alpha)$ 上不可约, $[L:\mathbb{Q}]=3\cdot2=6$. 由 $\gamma^3+9\gamma-2=3\beta(\gamma^2+1)$ 且 $3(\gamma^2+1)\neq0$, 得 $\beta=(\gamma^3+9\gamma-2)/(3(\gamma^2+1))\in\mathbb{Q}(\gamma)$, 于是 $\alpha=\gamma-\beta\in\mathbb{Q}(\gamma)$, 故 $L=\mathbb{Q}(\alpha,\beta)\subseteq\mathbb{Q}(\gamma)\subseteq L$, 即 $\mathbb{Q}(\gamma)=L$, $[\mathbb{Q}(\gamma):\mathbb{Q}]=6$. 所以 $\deg f=6$ 且 f 是 γ 的极小多项式, 不可约.

f 在 $\mathbb{C}$ 中的根即 γ 的共轭: γ 的共轭由 α 的共轭 $\omega^k\alpha$ ($\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$, $k=0,1,2$) 与 β 的共轭 $\pm\beta$ 组合而成, 即

$$\sqrt[3]{2}\pm\sqrt{3},\qquad \omega\sqrt[3]{2}\pm\sqrt{3},\qquad \omega^2\sqrt[3]{2}\pm\sqrt{3}.$$

(b) 设 $E=\mathbb{Q}(\alpha,\omega)$ 为 x^3-2 在 $\mathbb{Q}$ 上的分裂域, $F=\mathbb{Q}(\sqrt{3})$ 为 x^2-3 的分裂域, 则 $K=E\cdot F$. $\mathrm{Gal}(E/\mathbb{Q})\cong S_3$ (判别式 $\Delta(x^3-2)=-108$ 非平方, 见习题 8.2), $[E:\mathbb{Q}]=6$; $\mathrm{Gal}(F/\mathbb{Q})\cong\mathbb{Z}/2$.

求 $E\cap F$: $E=\mathbb{Q}(\alpha)(\omega)$ 是 $\mathbb{Q}(\alpha)$ 的二次扩域, 其最大实子域为 $\mathbb{Q}(\alpha)$. 若 $\sqrt{3}\in E$, 因 $\sqrt{3}\in\mathbb{R}$, 则 $\sqrt{3}\in\mathbb{Q}(\alpha)$, 与上面结论矛盾. 故 $E\cap F=\mathbb{Q}$.

两个 Galois 扩张 $E/\mathbb{Q}$, $F/\mathbb{Q}$ 的交为 $\mathbb{Q}$ 时, 复合域 K 的 Galois 群同构于直积, 故

$$\mathrm{Gal}(K/\mathbb{Q})\cong\mathrm{Gal}(E/\mathbb{Q})\times\mathrm{Gal}(F/\mathbb{Q})\cong S_3\times\mathbb{Z}/2,$$

阶为 12.

习题 8.4

Let $K=\mathbb{Q}(\alpha)$, where α is a root of the polynomial x^3+2x+1, and let $g(x)=x^3+x+1$. Does $g(x)$ have a root in K?

解答

题目翻译: 设 $K=\mathbb{Q}(\alpha)$, 其中 α 是多项式 x^3+2x+1 的根, 又设 $g(x)=x^3+x+1$. $g(x)$ 在 K 中有根吗?

解答: 没有.

设 $f(x)=x^3+2x+1$. f 无有理根 (±1 代入均非零), 故不可约, $[K:\mathbb{Q}]=3$, 且 $\{1,\alpha,\alpha^2\}$ 为 K 在 $\mathbb{Q}$ 上的基. $g(x)=x^3+x+1$ 也无有理根, 不可约.

反设 g 在 K 中有根 β. 因 g 不可约且 $\deg g=3=[K:\mathbb{Q}]$, 有 $\mathbb{Q}(\beta)=K$, 故 β 是 K 的本原元, 可写 $\beta=a+b\alpha+c\alpha^2$ $(a,b,c\in\mathbb{Q})$, 且 g 是 β 的极小多项式.

设 $\sigma_1=\mathrm{id}$, σ_2, σ_3 是 K 到 $\mathbb{C}$ 的三个嵌入, 满足 $\sigma_i(\alpha)=\alpha_i$, 其中 $\alpha_1,\alpha_2,\alpha_3$ 为 f 的三个根. 则 g 的三个根恰为

$$\beta_i=\sigma_i(\beta)=a+b\alpha_i+c\alpha_i^2 \qquad (i=1,2,3).$$

于是

$$\beta_i-\beta_j=b(\alpha_i-\alpha_j)+c(\alpha_i^2-\alpha_j^2)=(\alpha_i-\alpha_j)\Big(b+c(\alpha_i+\alpha_j)\Big).$$

由判别式的定义 ($\Delta=\prod_{i<j}(\text{根差})^2$) 得

$$\Delta_g=\prod_{i<j}(\beta_i-\beta_j)^2=\Delta_f\cdot\left(\prod_{i<j}\Big(b+c(\alpha_i+\alpha_j)\Big)\right)^2,$$

其中 $\Delta_f=\prod_{i<j}(\alpha_i-\alpha_j)^2$ 为 f 的判别式. 而 $r=\prod_{i<j}(b+c(\alpha_i+\alpha_j))$ 是 $\alpha_1,\alpha_2,\alpha_3$ 的对称多项式, 由对称多项式基本定理它等于其初等对称多项式 (即 f 的系数) 的有理系数多项式, 故 $r\in\mathbb{Q}$. 因此 $\Delta_g/\Delta_f=r^2$ 是有理数平方.

但 $f(x)=x^3+2x+1$ 的判别式为 $\Delta_f=-4\cdot2^3-27\cdot1^2=-59$, $g(x)=x^3+x+1$ 的判别式为 $\Delta_g=-4\cdot1^3-27\cdot1^2=-31$, 故 $\Delta_g/\Delta_f=31/59$. 而 31 与 59 都不是有理数平方, $31/59$ 不是有理数平方, 矛盾.

所以 $g(x)$ 在 K 中没有根.

7

第七次作业

习题 5.1

For each of the following sets of automorphisms of the field of rational functions $\mathbb{C}(t)$, determine the group of automorphisms that they generate, and determine the fixed field explicitly.
(a) $\sigma(t) = t^{-1}$
(b) $\sigma(t) = \mathrm{i}t$
(c) $\sigma(t) = -t$, $\tau(t) = t^{-1}$
(d) $\sigma(t) = \omega t$, $\tau(t) = t^{-1}$, where $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$.

解答 习题 5.1

题目翻译: 对有理函数域 $\mathbb{C}(t)$ 的下列各组自同构, 确定它们生成的自同构群, 并具体给出该群的不动域.
(a) $\sigma(t) = t^{-1}$, 与第六次作业习题 5.1 (a) 相同, 解答见上文.
(b) $\sigma(t) = \mathrm{i}t$, 与第六次作业习题 5.1 (b) 相同, 解答见上文.
(c) $\sigma(t) = -t$, $\tau(t) = t^{-1}$. 两者均为二阶对合: $\sigma^2 = 1$, $\tau^2 = 1$. 又

$$\sigma\tau(t) = \sigma(t^{-1}) = -t^{-1}, \qquad \tau\sigma(t) = \tau(-t) = (-t)^{-1} = -t^{-1},$$

故 $\sigma\tau = \tau\sigma$, 二者交换. 生成的群为 $\{1, \sigma, \tau, \sigma\tau\}$, 其中 $\sigma\tau : t \mapsto -t^{-1}$ 亦为二阶. 因此它是 Klein 四元群 $V_4 \cong C_2 \times C_2$.
不动域. 被 σ 固定的有理函数恰为 t^2 的有理函数, 故 $\mathbb{C}(t)^{\langle\sigma\rangle} = \mathbb{C}(t^2)$. 在 $\mathbb{C}(t^2)$ 上 τ 诱导 $s \mapsto s^{-1}$, 其中 $s = t^2$. $\mathbb{C}(s)$ 在 $s \mapsto s^{-1}$ 下的不动域为 $\mathbb{C}(s + s^{-1})$, 因而整个群的不动域为

$$\mathbb{C}(t)^{\{1,\sigma,\tau,\sigma\tau\}} = \mathbb{C}(t^2 + t^{-2}).$$

事实上 $[\mathbb{C}(t) : \mathbb{C}(t^2)] = 2$, 且 s 满足 $X^2 - (s+s^{-1})X + 1 = 0$, 故 $[\mathbb{C}(t^2) : \mathbb{C}(t^2+t^{-2})] = 2$, 总次数 $4 = |V_4|$, 与 Artin 引理一致.
(d) $\sigma(t) = \omega t$, $\tau(t) = t^{-1}$, 其中 $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$. 此处 $\sigma^3 = 1$, $\tau^2 = 1$, 且

$$\tau\sigma(t) = \tau(\omega t) = (\omega t)^{-1} = \omega^{-1}t^{-1} = \omega^2 t^{-1}, \qquad \sigma^2\tau(t) = \sigma^2(t^{-1}) = \omega^2 t^{-1},$$

故 $\tau\sigma = \sigma^2\tau$. 生成的群为 $\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, 满足 $\sigma^3 = \tau^2 = 1$ 与 $\tau\sigma = \sigma^2\tau$, 这是六阶二面体群 D_3, 同构于对称群 S_3.

不动域. 三阶子群 $\langle\sigma\rangle$ 的不动域为 $\mathbb{C}(t^3)$, 因 t 在 $\langle\sigma\rangle$ 下的轨道为 $\{t,\omega t,\omega^2 t\}$ 且 t^3 不变. 令 $s=t^3$, τ 诱导 $s\mapsto s^{-1}$, 从而整个群的不动域为 $\mathbb{C}(s+s^{-1})=\mathbb{C}(t^3+t^{-3})$. 次数 $[\mathbb{C}(t):\mathbb{C}(t^3)]=3$, $[\mathbb{C}(t^3):\mathbb{C}(t^3+t^{-3})]=2$, 总次数 $6=|D_3|$, 与 Artin 引理一致.

习题 5.2

Show that the automorphisms $\sigma(t)=(t+\mathrm{i})/(t-\mathrm{i})$ and $\tau(t)=(\mathrm{i}t-\mathrm{i})/(t+1)$ of $\mathbb{C}(t)$ generate a group isomorphic to the alternating group A_4, and determine the fixed field of this group.

解答 习题 5.2

题目翻译: 证明 $\mathbb{C}(t)$ 的两个自同构 $\sigma(t)=(t+\mathrm{i})/(t-\mathrm{i})$ 与 $\tau(t)=(\mathrm{i}t-\mathrm{i})/(t+1)$ 生成一个与交错群 A_4 同构的群, 并确定该群的不动域.
与第六次作业习题 5.2 相同, 解答见上文.

习题 6.2

Let $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Determine $[K:\mathbb{Q}]$, prove that K is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

解答 习题 6.2

题目翻译: 设 $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. 求 $[K:\mathbb{Q}]$, 证明 K 是 $\mathbb{Q}$ 的 Galois 扩张, 并确定其 Galois 群.
与第六次作业习题 6.2 相同, 解答见上文.

习题 6.3

Let $K\supset L\supset F$ be a chain of extension fields of degree 2. Show that K can be generated over F by the root of an irreducible quartic polynomial of the form x^4+bx^2+c.

解答 习题 6.3

题目翻译: 设 $K\supset L\supset F$ 是次数为 2 的域扩张链. 证明 K 可由 F 上形如 x^4+bx^2+c 的不可约四次多项式的根生成.
与第六次作业习题 6.3 相同, 解答见上文.

习题 7.3

How many intermediate fields L with $[L:F]=2$ are there when K/F is a Galois extension with Galois group (a) the alternating group A_4, (b) the dihedral group D_4?

解答　习题 7.3

题目翻译: 设 K/F 是 Galois 群为下述群的 Galois 扩张, 问满足 $[L:F]=2$ 的中间域 L 有多少个? (a) 交错群 A_4, (b) 二面体群 D_4.
与第六次作业习题 7.3 相同, 解答见上文.

习题 7.6

Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is K the splitting field of an irreducible cubic polynomial over F?

解答　习题 7.6

题目翻译: 设 K/F 的 Galois 群为对称群 S_3. 问 K 是否为 F 上某个不可约三次多项式的分裂域?
与第六次作业习题 7.6 相同, 解答见上文.

习题 7.7

(a) Determine the irreducible polynomial for $\mathrm{i}+\sqrt{2}$ over $\mathbb{Q}$. (b) Prove that the set $\{1,\mathrm{i},\sqrt{2},\mathrm{i}\sqrt{2}\}$ is a basis for $\mathbb{Q}(\mathrm{i},\sqrt{2})$ over $\mathbb{Q}$.

解答　习题 7.7

题目翻译:(a) 求 $\mathrm{i}+\sqrt{2}$ 在 $\mathbb{Q}$ 上的不可约多项式. (b) 证明集合 $\{1,\mathrm{i},\sqrt{2},\mathrm{i}\sqrt{2}\}$ 是 $\mathbb{Q}(\mathrm{i},\sqrt{2})$ 在 $\mathbb{Q}$ 上的一组基.
与第六次作业习题 7.7 相同, 解答见上文.

习题 7.10

Let K/F be a Galois extension with Galois group G, and let H be a subgroup of G. Prove that there exists an element $\beta\in K$ whose stabilizer is equal to H.

解答　习题 7.10

题目翻译: 设 K/F 是 Galois 群为 G 的 Galois 扩张, H 是 G 的一个子群. 证明存在元素 $\beta\in K$ 使其稳定子恰等于 H.
与第六次作业习题 7.10 相同, 解答见上文.

习题 7.5

Let $f(x)$ be an irreducible cubic polynomial over $\mathbb{Q}$ whose Galois group is S_3. Determine the possible Galois groups of the polynomial $(x^3-1)f(x)$.

解答　习题 7.5

题目翻译: 设 $f(x)$ 是 $\mathbb{Q}$ 上 Galois 群为 S_3 的不可约三次多项式. 求多项式 $(x^3-1)f(x)$ 可能的 Galois 群.
与第六次作业习题 7.5 相同, 解答见上文.

习题 7.11

Let $\alpha = \sqrt[3]{2}$, $\beta = \sqrt{3}$, and $\gamma = \alpha + \beta$. Let L be the field $\mathbb{Q}(\alpha, \beta)$, and let K be the splitting field of the polynomial $(x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$. (a) Determine the irreducible polynomial f for γ over $\mathbb{Q}$, and its roots in $\mathbb{C}$. (b) Determine the Galois group of $K/\mathbb{Q}$.

解答　习题 7.11

题目翻译: 设 $\alpha = \sqrt[3]{2}$, $\beta = \sqrt{3}$, $\gamma = \alpha+\beta$. 令 $L = \mathbb{Q}(\alpha, \beta)$, K 是多项式 $(x^3-2)(x^2-3)$ 在 $\mathbb{Q}$ 上的分裂域. (a) 求 γ 在 $\mathbb{Q}$ 上的不可约多项式 f 及其在 $\mathbb{C}$ 中的根. (b) 求 $K/\mathbb{Q}$ 的 Galois 群.
与第六次作业习题 7.11 相同, 解答见上文.

习题 8.2

Determine the Galois groups of the following polynomials over $\mathbb{Q}$: (a) $x^3 - 2$, (b) $x^3+3x+14$, (c) x^3-3x^2+1, (d) $x^3-21x+7$, (e) x^3+x^2-2x-1, (f) x^3+x^2-2x+1.

解答　习题 8.2

题目翻译: 求下列多项式在 $\mathbb{Q}$ 上的 Galois 群: (a) x^3-2, (b) $x^3+3x+14$, (c) x^3-3x^2+1, (d) $x^3 - 21x + 7$, (e) $x^3 + x^2 - 2x - 1$, (f) $x^3 + x^2 - 2x + 1$.
与第六次作业习题 8.2 相同, 解答见上文.

习题 8.4

Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial x^3+2x+1, and let $g(x) = x^3+x+1$. Does $g(x)$ have a root in K?

解答　习题 8.4

题目翻译: 设 $K = \mathbb{Q}(\alpha)$, 其中 α 是多项式 $x^3 + 2x + 1$ 的根, 令 $g(x) = x^3 + x + 1$. 问 $g(x)$ 在 K 中是否有根?
与第六次作业习题 8.4 相同, 解答见上文.