A. И. 柯斯特利金《代数学引论》第三卷习题提示暨勘误

中国科学院数学与系统科学研究院

李文威

wwli@math.ac.cn

版本: 2018-01-02

INTERVIEWER Some people say they can't understand your writing, even after they read it two or three times. What approach would you suggest for them?

FAULKNER Read it four times.

William Faulkner, The Art of Fiction No. 12
The Paris Review, No. 12, Spring 1956.

凡例

呈献给读者的是笔者于 2015, 2017 年秋季学期, 在中国科学院大学[1]为大二本科生讲授代数学时, 应要求为课本《代数学引论》第三卷[2]编撰的习题提示以及部分改正. 因事出匆忙, 错漏在所难免, 在此祈求方家斧正. 虽是野人献曝, 倘若这份资料对研读《代数学引论》汉译本的广大师生能有一丝一毫的助益, 笔者的绵薄之力便有所值了.

编撰原则简述如下:

- 基于授课时的现实, 我们不求覆盖所有章节.

[1] 玉泉路校区, 北京市石景山区.
[2] 第二版, A. И. 柯斯特利金著; 郭文彬译. (北京: 高等教育出版社, 2007 年, ISBN 978-7-04-022506-8)

- 如书上已有提示,并且对解题有实质帮助者,则不再多言.
- 纯计算类的题目略去提示,不过这类题目在书中并不多.
- 书里一些习题既无计算,亦非证明,更不能归为思考题,只能说是 А. И. Кострикин 作的一些评注或发挥. 这类习题当然无需提示.
- 引用的页码和结果如无另外申明,则一概指向课本. 我们有时也沿用原书体例,以 [BAI], [BAII], [BAIII] 代表《代数学引论》汉译本的一至三卷.
- 我们基本遵循《代数学引论》的符号,但考量到当今数学界通用的符号或有不同,仍有少量改动. 惯例如下:
  - 以 $|E|$ 或 $\#E$ 表集合 E 的元素个数;
  - 以 $\mathbb{Z}/n\mathbb{Z}$ 表 n 个元素的循环群;
  - 环 R 皆含幺元,其乘法可逆元构成的群记为 $R^\times$;
  - 群 G 的运算如以乘法表示,不致混淆时记 G 的幺元为 1. 类似地, $n \times n$ 单位矩阵记为 1_n 或 1;
  - 群 G 的中心记为 $Z(G)$,类似地环或代数 R 的中心记为 $Z(R)$;
  - 代数结构 (群,模等等) 的同态集记为 Hom,自同态集记为 End,自同构集记为 Aut;
  - 整数的同余式写作 $x \equiv a \pmod n$ 之形.
- 超链接可以在各式 PDF 阅览器中点击.

勘误

以下仅限于本人所能发现并且记得的错误.

- $\boxed{\text{§1.4 最后一段}}$ 应指 "流形的基本群".
- $\boxed{\text{§2.2 习题 4}}$ ... 后者成立的必要条件是 $p \mid (q-1)$.
- $\boxed{\text{§5.4.2, 命题 2 的证明}}$ 更正确的论证如下. 根据条件, G 含有一个对换和一个 p-循环 σ. 因为 p 为素数, p 阶元必为 p-循环. 用 S_p 中的适当元素对 G 共轭后,可设对换为 (12). 存在 $s \in \mathbb{Z}$ 使得 $\sigma^s(1) = 2$,这时 σ^s 仍是 $\langle\sigma\rangle$ 的生成元,故仍是 p-循环,形如 $(12a_3 \cdots a_p)$,其中 $\{a_3, \ldots, a_p\} = \{3, \ldots, p\}$. 再用 S_p 中保持 $1, 2$ 不动而映 $i \mapsto a_i$ 的元素对 G 共轭,可设 $\eta := \sigma^s = (123 \cdots p)$. 于是精确到共轭, G 含 $\eta(12)\eta^{-1} = (23)$, $\eta(23)\eta^{-1} = (34)$,依此类推,得到 S_p 的标准生成集落在 G 中.

- $\boxed{\text{§5.5.1 定理 1 的证明}}$ 正确论证如下. 对正整数 m 的因子个数作归纳, 可从 $X^m - 1 = \prod_{d|m} \Phi_d$ 推得整系数首一多项式 Φ_m 的常数项在 $m = 1$ 时为 -1, 否则为 1. 以下用归谬法. 设满足 $p \equiv 1 \pmod n$ 的素数 p 仅有有限个, 记为 $\{p_1, \ldots, p_s\}$. 那么根据先前的引理 2, 对任意整数 a, 素数 p 整除 $\Phi_n(a)$ 蕴涵 $\exists i \; p = p_i$. 现在取 $a = (p_1 \cdots p_s)^N$, $N \gg 0$, 那么 $\Phi_n(a) > 1$, 而且对每个 i 都有 $\Phi_n(a) \equiv 1 \pmod{p_i}$, 故 $\Phi_n(a)$ 有 $p_1, \ldots, p_s$ 之外的素因子. 矛盾.
- $\boxed{\text{§5.5.5 定理 13}}$ 关于实根式解的讨论, 较好的文献是 I. M. Issacs, Solution of polynomials by real radicals. The American Mathematical Monthly, Vol 92, No 8 (1985). pp.571–575.

§1.1

1. 直接计算.
2. 直接计算.
3. 透过 Γ, 它们分别对应到 Q_8 的元素 ± 1, $\pm\mathbf{i}$, $\pm\mathbf{j}$ 和 $\pm\mathbf{k}$, 四元数的乘法对应到矩阵乘法.
4. 无可能. 因为 $\mathbb{C}$ 将透过左乘使得 A 成为 $\mathbb{C}$-向量空间, 而且 $\mathbb{R}$-代数的结构将导致

$$\dim_{\mathbb{R}} A = 2 \dim_{\mathbb{C}} A,$$

故 $\dim_{\mathbb{R}} A$ 必为偶数.

5. 略.

§1.2

1. 设 $H \subset G$ 指数为 2, 以下证明 $Hx = xH$ 对所有 x 都成立. 留意到 $Hx = H \iff x \in H$. 若 $x \in H$ 则 $Hx = H = xH$. 又由于无交并分解中仅有两项, 若 $x \notin H$ 则 $Hx = G \smallsetminus H$; 同理, 这也给出唯一的陪集 xH, 综之亦有 $Hx = xH$.
2. 设 G 为 6 阶群. 根据 Cauchy 定理, 存在 3 阶元 σ 和二阶元 τ; 这点也可以如下验证:
   - 因为 $|G|$ 为偶数, 考察 $x \mapsto x^{-1}$ 的不动点可知必有二阶元 τ;
   - 若所有元素 $\neq 1$ 都是二阶, 则 $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ 导致 G 交换, 矛盾.

由 $\langle\sigma\rangle \lhd G$ 可证明 $\tau\sigma = \sigma^{\pm 1}\tau$, 从而 G 中形如

$$\tau^i\sigma^j, \quad i = 0, 1,\ j = 0, 1, 2$$

的元素构成子群 G_0. Lagrange 定理导致 $\langle\sigma\rangle \cap \langle\tau\rangle = \{1\}$, 故此表法唯一, 从而 $G_0 = G$. 假若 $\tau\sigma\tau^{-1} = \sigma$ 则 G 交换, 否则 $\tau\sigma\tau^{-1} = \sigma^{-1}$, 这时我们得到 S_3 的乘法: 例如取 $\tau = (1, 2)$, $\sigma = (1, 2, 3)$.

§1.3

1. 对于任意 x, 轨道 $G(x)$ 等价于 $G/\mathrm{St}(x)$, 办法是映 gx 为 $g\mathrm{St}(x)$.

2. 设 $|G| = p^2$, 则中心 $Z \neq \{1\}$. 若 $|Z| = p^2$ 则 G 交换, 否则 $|Z| = p$. 这时存在 p 阶元 $x \notin Z$. 可以证明
$$x^a \in Z \iff p \mid a$$
(考虑使此式成立的最小 $a \geq 1$; 所有其它 a 都被它整除.) 因此陪集分解给出 $G = \bigcup_a x^a Z$, 由此立见 G 交换.

3. 见课本提示.

4. 见课本提示.

5. 初等组合学.

6. 平凡的. 注意到 “最小不变子群” 应改为 “最小不变子集”.

7. 略.

8. 见课本提示, 或用以下方法: 作分解 $\Omega = \Omega_1 \sqcup \Omega_2 \sqcup \cdots$ 使得每个 Ω_i 都是可迁不变子集, 相应地 $N(g) = N_\Omega(g)$ 分解为 $\sum_i N_{\Omega_i}(g)$. 于是化约到 Ω 可迁的情形, 此时 $r(G : \Omega) = 1$. 这无非是定理 3.

9. 如果 $a^2 = 1$ 则 $D(a) = \{x : xa = ax\} = C(a)$ 是群. 反之设 $D(a)$ 是群, 从 $1 \in D(a)$ 立见 $a^2 = 1$. 一般情形下, 容易验证
$$D(a)D(a) \subset C(a),\ C(a)D(a) \subset D(a),\ D(a)C(a) \subset D(a),\ D(a)^{-1} \subset D(a)$$
因此 $C(a) \cup D(a)$ 总是一个子群.

§1.4

1. 以 $\mathrm{Ad}(g)$ 记内自同构 $x \mapsto gxg^{-1}$, 则对任意自同构 σ 都有 $(\sigma\mathrm{Ad}(g)\sigma^{-1})(x) = \sigma(g)x\sigma(g)^{-1} = \mathrm{Ad}(\sigma(g))(x)$. 故 $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.
2. 考虑满射 $(h,k) \mapsto hk$, 证明它的每一条 "纤维" 都恰有 $|H \cap K|$ 个元素. 其余略去.
3. 略.
4. 平凡.
5. 正确, 考虑显然的同态 $G \to G/K_1 \times G/K_2$, 其核为 $K_1 \cap K_2$.
6. 假设 $K \cap A = K \cap B = \{1\}$. 在 [BAIII, §1.4 定理 6] 的证明中已隐含以下一般性质

   $$N_1, N_2 \lhd G,\ N_1 \cap N_2 = \{1\} \implies \forall (x,y) \in N_1 \times N_2,\ xy = yx.$$

   应用于 $N_1 = K$, $N_2 = A, B$, 得到 $K \subset Z_G(A) \cap Z_G(B)$, 这里 $Z_G(\cdots)$ 代表中心化子群. 于是 K 包含于 $A \times B$ 的中心.
7. 不是. 事实上考虑 Q_8 的循环子群即知所有非平凡子群都包含 $\{\pm 1\}$, 故不可能分解为半直积.
8. 应用上述观察和 [BAIII, §1.4, 定理 4] (正规子群的对应定理, 此处取 $K = \{\pm 1\}$).
9. 应用上题结果: D_4 有非正规子群 (例如二阶子群 $\langle \mathscr{B} \rangle$), Q_8 则否.
10. 分别考虑自同构在生成元 $\mathscr{A}$ 和 $\mathscr{B}$ 上的效应.
11. 略.
12. 见课本提示.
13. 对 $\sigma \in S_n$, 定义 $f(\sigma)$ 为以下线性变换: $e_i \mapsto e_{\sigma(i)}$, 其中 $e_1, \ldots, e_n \in F^n$ 是一组基. 更具体的方法请见课本提示.
14. 见任一本代数教材, 如聂灵沼, 丁石孙《代数学引论》第二版 (北京: 高等教育出版社, 2000 年), §2.11.

§2.1

1. 略
2. 设 $|G| = p^n$. 当 $n \geq 1$ 时 p.17 定理 2 蕴含中心 $Z(G) \neq \{1\}$. 对 n 作数学归纳法可知 $G/Z(G)$ 和 $Z(G)$ 都可解.

3. 略

4. 若子群 $H \subset A_5$ 满足 $|H| = 15$, 由 §2.2 习题 4 知 H 为循环群, 这在 A_5 中不可能.

   若 $|H| = 20$, 则由 A_5 的单性可知正规化子群 $N_{A_5}(H) = H$. 先观察到 H 必包含形如 $(ab)(cd)$ 的 2 阶元. 任取 5 阶元 $\tau \in A_5$, 令 $\langle\tau\rangle \simeq \mathbb{Z}/5\mathbb{Z}$ 以共轭方式作用于 A_5/H; 说明这是平凡作用, 故 H 包含所有 5-循环. 由等式

$$(abcde)(ab)(cd) = (ace) \notin H$$

   导出矛盾.

§2.2

1. 设素数 $p > 2$, 视 S_p 为同余类集 $\mathbb{Z}/p\mathbb{Z}$ 上的置换群. 则 S_p 中的 Sylow p-子群 (必包含于 A_p) 由 $(12\cdots p)$ 生成, 元素为形如 $a \mapsto a+i$ 的映射; 说明其正规化子群由如下映射组成

$$1 \mapsto k, \quad 2 \mapsto k+i, \quad 3 \mapsto k+2i, \ldots$$

   其中 $k \in \mathbb{Z}/p\mathbb{Z}$ 而 $(i,p) = 1$; 共有 $p(p-1)$ 种选法. 所以 Sylow p-子群的个数 $N_p = \frac{p!}{p(p-1)} = (p-2)!$.

2. 略

3. 比较中心可知 $S_4 \not\simeq \mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$. 现在解释 $A_4 \simeq \mathrm{PSL}(2, \mathbb{Z}/3\mathbb{Z})$ 的缘由. 先说明两边都有正规的 Sylow 2-子群 $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 由此说明两边都可写成 Sylow 2-子群与 3-子群的半直积. 具体选取 3 阶元如 $\left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$ 以说明在同构意义下, 两个半直积由相同的同态 $\mathbb{Z}/3\mathbb{Z} \hookrightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ 确定.

4. 注意: 本题的 $p \nmid q-1$ 仅是 G 非交换的必要条件, 非充分 (因为对任何 $p < q$ 都可以取 $G = \mathbb{Z}/pq\mathbb{Z}$). 设 P, Q 分别为 Sylow p- 和 q-子群, 用 Sylow 第三定理导出 $N_G(Q) = G$ 和半直积 $G = Q \rtimes P$. 群 G 的结构由共轭作用导出的同态

$$\mathbb{Z}/p\mathbb{Z} \simeq P \to \mathrm{Aut}(Q)$$

   确定, 当此同态平凡时 $G = P \times Q$. 说明 $\mathrm{Aut}(Q) \simeq \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ 为 $q-1$ 阶群, 由此导出 $p \nmid q-1 \implies G \simeq P \times Q$ 是循环群.

5. 利用第一题的提示.

6. 首先排除 $|G| = p^n$ 或 $|G| = pq$ 情形, 其中 p, q 是素数. 剩余情形如下.

- $|G| = 2^2 \cdot 3$: 若 Sylow 2-子群 P 非正规, 必有 $N_2 := (G : N_G(P)) = (G : P) = 3$; 此式对所有 Sylow 2-子群皆成立. 说明 $P^\flat := \bigcap_{g \in G} gPg^{-1} \lhd G$, 而且 G 在 $\{P' \subset G : \text{Sylow 2-子群}\}$ 上的共轭作用将 $G/P^\flat$ 嵌入 S_3. 由 $|S_3| < |G|$ 导出 $P^\flat \neq \{1\}, G$, 从而证明 G 非单.
- $|G| = 2 \cdot 3^2$: 证明 Sylow 3-子群正规.
- $|G| = 2^2 \cdot 5$: 证明 Sylow 5-子群正规.
- $|G| = 2^3 \cdot 3$: 同 $|G| = 2^2 \cdot 3$ 情形类似, 考虑 Sylow 2-子群 P 非正规的情形.
- $|G| = 2^2 \cdot 7$: 证明 Sylow 7-子群正规.
- $|G| = 2 \cdot 3 \cdot 5$: 见课本提示.

§2.3

1. 略
2. 化约到 A 是 p-群情形, 其中 p 是素数. 注意到 $\forall j \geq 0$

$$B \leq A \implies p^j B \leq p^j A \implies (p^j B)[p] \leq (p^j A)[p],$$

   其中 $(\cdots)[p]$ 表示交换群的 p-挠部分, 然后回顾不变量的唯一性证明.
3. 化约到 A, B 皆为 p-群的情形, 其中 p 是素数, 然后使用不变量.
4. 同上.
5. 略
6. 略
7. 略
8. 略
9. 使用定理 2.

§2.4

1. 见课本提示.
2. 至少有两种方法.

- 先推出 $\mathscr{D}^n[\mathbf{a},\mathbf{b}] = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}[\mathscr{D}^k\mathbf{a}, \mathscr{D}^{n-k}\mathbf{a}]$, 代入 $\exp(\mathscr{D}) = \sum_{n=0}^{\infty} \frac{\mathscr{D}^n}{n!}$ 以证明

$$\exp(\mathscr{D})[\mathbf{a},\mathbf{b}] = \sum_{u=0}^{\infty}\sum_{v=0}^{\infty} \frac{[\mathscr{D}^u\mathbf{a}, \mathscr{D}^v\mathbf{b}]}{u!v!} = [\exp(\mathscr{D})\mathbf{a}, \exp(\mathscr{D})\mathbf{b}].$$

  收敛性不成问题.

- 考虑向量值函数

$$\mathbb{R} \xrightarrow{\Phi_1,\Phi_2} \{\text{双线性映射 } L(G)\times L(G) \to L(G)\} \simeq \mathbb{R}^{(\dim L(G))^2+\dim L(G)}$$

$$\begin{aligned}\Phi_1(s)(\mathbf{a},\mathbf{b}) &= \exp(s\mathscr{D})[\mathbf{a},\mathbf{b}]\\ \Phi_2(s)(\mathbf{a},\mathbf{b}) &= \left[\exp(s\mathscr{D})\mathbf{a}, \exp(s\mathscr{D})\mathbf{b}\right].\end{aligned}$$

  验证两者皆满足一阶线性常微分方程 + 初值条件

$$\begin{gathered}\Phi_i'(s)(-,-) = \Phi_i(s)(\mathscr{D}(-),-) + \Phi_i(s)(-,\mathscr{D}(-)),\\ \Phi_i(0) = [-,-], \quad i=1,2.\end{gathered}$$

  从而导出 $\forall s,\ \Phi_1(s) = \Phi_2(s)$.

§3.1

1. 直接验证.

2. 皆不可约. 如果不用更深入的理论, $n=3$ 的情形将十分繁琐...

3. 取定 n 阶循环群 A. 先注意到 Φ, Ψ 必然是一维的. 当 $\Phi \simeq \Psi$ 时显然

$$\frac{1}{n}\sum_{a\in A} \Phi(a)\overline{\Psi(a)} = 1.$$

   若 $\Phi \neq \Psi$, 取 b 使得 $\Phi(b) \neq \Psi(b)$, 并在 $\frac{1}{n}\sum_{a\in A}\Phi(a)\overline{\Psi(a)}$ 中以 ab 代 a 来论证.

4. 取定 n 阶循环群 A 及其生成元 a. 上题的配对 $(\Phi,\Psi) \mapsto \frac{1}{n}\sum_{k=0}^{n-1}\Phi(a)\overline{\Psi(a)}$ 给出函数空间 $\{\Phi : A \to \mathbb{C}\} \simeq \mathbb{C}^n$ 上的非退化 Hermite 型. 仅须证明函数族 $\left\{a^k \mapsto \varepsilon^{km}\right\}_{m=0}^{n-1}$ 对之构成标准正交基 (见 [BAII, 第 3 章 §2]).

5. 对第一小题可延续课本思路: 将 q 种颜色的珠子循序排在 p 个位置上, p 为素数, 共有 q^p 种排法. 群 $\mathbb{Z}/p\mathbb{Z} \subset S_p$ 透过轮换重置这些排列. 在 p-轮换下不变的

排法只能是同色排列, 共 q 种. p-群作用下的计数公式 (参看课本 p.17) 遂给出 $q^p \equiv |同色排列| = q \pmod p$.

对于第二小题, 在课本 p.71 公式 (**) 中取 $q = 1$ 即是.

§3.2

1. 关于酉性的部分可直接验证. 至于 $(\mathbb{R}, +)$ 的一维连续表示的刻画, 这可以作为已知性质 (超纲), 也可以用拓扑学知识论证如下: 给定一维连续表示相当于给定拓扑群的连续同态 $\Phi : \mathbb{R} \to \mathbb{C}^\times$. 易见 $\mathbb{C}^\times$ 的万有覆叠空间作为拓扑群由

$$\begin{aligned} e : (\mathbb{C}, +) &\twoheadrightarrow (\mathbb{C}^\times, \cdot) \\ z &\mapsto \exp(iz), \quad \operatorname{Ker}(e) = 2\pi\mathbb{Z} \simeq \pi_1(\mathbb{C}^\times, 1), \end{aligned}$$

   给出, 故存在唯一的连续同态 $\tilde{\Phi} : (\mathbb{R}, +) \to (\mathbb{C}, +)$ 满足 $\Phi = e \circ \tilde{\Phi}$. 容易看出 $\exists! \alpha \in \mathbb{C}$ 使得 $\tilde{\Phi}(t) = \alpha t$, 相应地 $\Phi = \Phi^{(\alpha)}$.

2. 微积分习题.

3. 设 $\rho : G \hookrightarrow \mathrm{GL}(2, \mathbb{C})$ 是忠实二维表示. 若 ρ 可约则 Maschke 定理给出分解 $\mathbb{C}^2 = V \oplus W$, 其中 $\dim V = \dim W = 1$. 选取 V 和 W 的元素为基, 可见 ρ 的像必为对角矩阵, 故为交换群, 从而 G 亦交换.

§3.3

1. 根据题目提供的子群信息, $\mathbf{I}$ 至少包含了

$$\begin{gathered} 1 \text{ 个 } 1 \text{ 阶元}, \\ 15 \text{ 个 } 2 \text{ 阶元}, \\ 20 \text{ 个 } 3 \text{ 阶元}, \\ 24 \text{ 个 } 5 \text{ 阶元}. \end{gathered}$$

   其和为 $60 = |\mathbf{I}|$ 故穷尽了 $\mathbf{I}$. 现在考量共轭类.

   (a) 由于 2 阶子群皆共轭, 全体 2 阶元同属一个共轭类.

   (b) 选定 Sylow 3-子群 $S \simeq \mathbb{Z}/3\mathbb{Z}$, 由题目信息知 $|N_{\mathbf{I}}(S)| = 6$, 所以 $N_{\mathbf{I}}(S)$ 中存在角度为 π 的旋转 η, 它不可能与 S 中的所有元素交换, 否则 $\mathbf{I}$ 将有 6 阶元, 于是 η 在 S 上的共轭作用是 $s \mapsto s^{-1}$. 综上可知全体 3 阶元共轭.

(c) 准此要领, 选定 Sylow 5-子群 $W \simeq \mathbb{Z}/5\mathbb{Z}$, 故 $N_{\mathbf{I}}(W)$ 的阶数为 10. 由此导出存在角度为 π 的旋转 $\tau \in N_{\mathbf{I}}(W)$, 它保持 W 中元素的公共转轴不变, 但不以 W 的轴为轴 (否则 $\mathbf{I}$ 将有十阶元), 因此 τ 在 W 上的作用为 $t \mapsto t^{-1}$. 这就看出 5 阶元的共轭类一一对应于 W 在 τ 作用下的轨道, 按转角分成 $\pm\pi/5$ 和 $\pm 4\pi/5$ 两类.

综之, 共有五个共轭类:

元素阶数	类的大小
1	1
2	15
3	20
5	12
5	12

若 $N \lhd \mathbf{I}$, 则 $|N| \mid 60$ 并且 $|N| - 1$ 可表为 15, 20, 12, 12 的和, 容易验证 $|N| = 1$.

2. 纯代数的方法是利用 60 阶单群的唯一性, 这是熟知的性质, 见 Grouppops. 几何证明的梗概如下: 由 A_5 的单性和 §1.2 习题 1 可知 S_5 中 60 阶的子群必为 A_5, 故只须构造非平凡的同态 $\mathbf{I} \to S_5$. 在正 20 面体中取对边中点连线, 共有 15 条, 可以证明其中两两垂直的三元组共有 5 个. 而 $\mathbf{I}$ 重排这些三元组, 这就给出了 $\mathbf{I} \to S_5$. 等价的说法是: 正 20 面体自然地内接 5 个正 8 面体, 对称群 $\mathbf{I}$ 重排之.

3. 对 SO(3) 的情用定理 2 处理, 对于 $H \leq \mathrm{SU}(3)$ 的情形, 注意到 H 到它在 SO(3) 中的像是同构.

4. 若 $H \leq \mathrm{SU}(2)$ 非逆像, 则 H 到 $\bar{H} \leq \mathrm{SO}(3)$ 为同构. 于是当 $|H|$ 为奇数时 $\bar{H}$ 中存在二阶元 τ (Cauchy 定理), 亦即角度为 π 的旋转. 然而易见这种旋转在 SU(2) 里的任一逆像 $\tilde{\tau}$ 阶满足 $\tilde{\tau}^2 = -1$, 矛盾.

5. 验证这两个元素在 SO(3) 中的像满足 D_3 的展示, 因而包含于 D_3^* (精确到共轭), 再验证它包含 -1 即可.

6. 它们同构, 见 Groupprops.

7. 见课本提示.

8. 应用几何性质: 四面体内接于四面体, 而八面体内接于立方体. 给外面着色相当于给内接顶点着色, 而且两者有相同的对称群.

§3.4

1. 见课本提示.
2. 直接计算, 回忆: $\Phi^{(3)}$ 是 S_3 在 $\mathbb{C}^3$ 上的置换表示 $e_i \mapsto e_{\sigma(i)}$ $(i = 1, 2, 3)$ 的不变子空间 $\left\{ae_1 + be_2 + ce_3 : a + b + c = 0\right\}$.
3. 见课本提示.
4. 当 τ 是内自同构 $x \mapsto gxg^{-1}$ 时, $\Phi^\tau \simeq \Phi$ 由 $\Phi(g)$ 实现.
5. 见课本提示.
6. 见课本提示.
7. 条件表明 Φ 和 Ψ 有相同的特征标. 应用定理 2 的推论.

§3.5

1. 作展开 $\Gamma_i = \sum_k (\Gamma_i|\chi_k)_G \chi_k = \sum_k \frac{|\Gamma_i|}{|G|} \chi_k(g_i)\chi_k$, 其中取定 $g_i \in \Gamma_i$. 特征标的第一正交关系和 $(\Gamma_i|\Gamma_j)_G = \frac{|\Gamma_i|}{|G|}\delta_{i,j}$ (使用 Kronecker 的 δ-符号) 遂导致

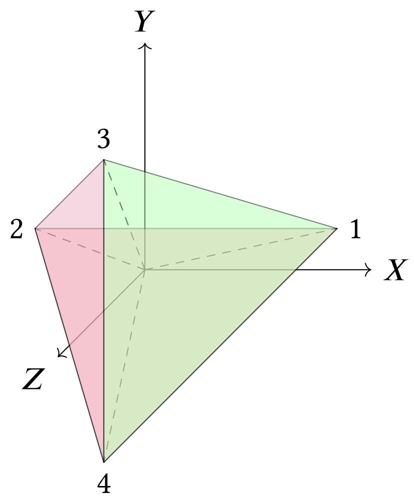
$$\begin{aligned} \frac{|\Gamma_i|}{|G|}\delta_{i,j} &= \sum_k t_{ik}\overline{t_{jk}} \\ &= \sum_k \frac{|\Gamma_i|}{|G|}\frac{|\Gamma_j|}{|G|}\chi_k(g_i)\overline{\chi_k(g_j)}. \end{aligned}$$

   由此可以导出 (4).

2. 见课本提示, 须假设 A 是有限交换群.
3. 忠实的复不可约表示无非是群的单同态 $\rho : A \hookrightarrow \mathbb{C}^\times$, 而 $\mathbb{C}^\times$ 的有限子群皆是循环群.
4. 一种办法是应用有限交换群的结构定理化约到 $A = \mathbb{Z}/n\mathbb{Z}$, $B = d\mathbb{Z}/n\mathbb{Z}$ 的情形, 这里 $d \mid n$.
5. 这里需要一些几何图像. 保持白磷分子不变的 $g \in O(3)$ 由它在四个磷原子 $\{1, 2, 3, 4\}$ 上的置换作用确定. 若只考虑旋转 $g \in SO(3)$, 则这给出群 $\mathbf{T}$ 到 A_4 的同构; 如容许 $\det g = -1$ 则得到 S_4 (见以下说明). 群 S_4 共有 5 个共轭类, 以下只看代表元的作用:
   - 恒等变换, 迹为 $3 = \dim \mathbb{R}^3$.

- (123): 取过顶点 4 和三角形 123 重心的连线为轴, 作角度为 $2\pi/3$ 的旋转, 这种旋转的迹为 $1+2\cos\frac{2\pi}{3}=0$ (参看第 10 题).
- (13)(24): 相对于共价键 13 和 24 中点连线作角度 π 的旋转. 这也是先做 (234) 再作 (134) 的结果. 这种旋转的迹为 $1+2\cos\pi=-1$.
- (12): 对一个包含 $\{3,4\}$ 的适当平面作镜射. 镜射的迹为 $1+1+-1=1$.
- (1234): 根据下一题可知 $\sum_g \mathrm{trace}(g)=0$, 直接计算可确定此元素的迹为 -1

这和 p.107 表的最后一行相符. 图片来源于TeX - LaTeX Stack Exchange.



6. 等于平凡表示在 χ 的不可约分解中出现的次数.
7. 见课本提示.
8. 略.
9. 略.
10. 略.

§3.6

1. 以 $P_n \supset H_n$ 表示 n 次三元齐次多项式及调和多项式构成的复向量空间. 定义线性单射

$$\begin{aligned} A: P_n &\longrightarrow P_{n+2} \\ f &\longmapsto (X^2+Y^2+Z^2)f. \end{aligned}$$

仅须证明 $P_{n+2}=A(P_n)\bigoplus H_n$ 即可导出 $\dim H_n=2n+1$. 为了做到这点, 赋予 P_n Hermite 内积使得

- 不同的单项式 $X^aY^bZ^c$ 相垂直,
- $\|X^aY^bZ^c\|^2 = a!b!c!$; 这里 $a+b+c=n$.

请验证此内积满足于

$$\left(Af\middle|g\right) = \left(f\middle|\Delta g\right), \quad f \in P_n,\ g \in P_{n+2}.$$

因此 $\Delta = {}^*A$, 于焉导出正交分解 $P_{n+2} = A(P_n) \bigoplus H_n$.

2. 见课本提示, 或利用上题之正交分解.

3. 按前一题将 $\tilde{g}$ 表为 $a_m h_m + a_{m-2}h_{m-2} + \cdots$ 之形, 其中 a_i 是 $X^2+Y^2+Z^2$ 的多项式, 而 a_j 是调和多项式. 限制在 $X^2+Y^2+Z^2=1$ 上即所求.

4. 如课本提示: 若 $\tau : \mathrm{SO}(3) \to \mathrm{SU}(2)$ 非平凡, 则因 SO(3) 是单群故 $\mathrm{Ker}(\tau)$ 必为平凡子群. 特别地, τ 给出 SO(3) 的二维忠实复表示. 因此我们得到二维忠实复表示 $S_4 \hookrightarrow \mathrm{SO}(3)$. 利用 p.107 的表可知 τ 或者 (a) 分解为两个一维表示的直和, 这与 SO(3) 非交换矛盾, 或者 (b) τ 对应到表中的特征标 χ_5, 然而该处业已说明此表示在 $V_4 \lhd S_4$ 上平凡, 故矛盾.

§3.7

1. 利用本节公式 (6), 亦即 $\chi_{V\otimes W} = \chi_V\chi_W$, 和 p.103 与 p.107 的特征表标直接计算.

2. 运用以下事实: 设 $\phi : G \to \mathbb{C}$ 和 $\psi : H \to \mathbb{C}$ 是共轭类上的函数, 由此以显然的方法构造 $\phi\psi : G \times H \to \mathbb{C}$, 它取值依然只和共轭类有关, 并且对 [BAIII, p.96] 的 Hermite 内积有
$$\|\phi\psi\|^2_{G\times H} = \|\phi\|^2_G\|\psi\|^2_H.$$
由此可以验证 V, W 不可约 $\implies \|\chi_V\|_G = \|\chi_W\|_H = 1 \implies \|\chi_{V\boxtimes W}\|_{G\times H} = 1$, 故 $V \boxtimes W$ 作为 $G \times H$ 的表示不可约. 同理
$$(\chi_V \mid \chi_{V'})_G(\chi_W \mid \chi_{W'})_H = \left(\chi_{V\boxtimes W}\middle|\chi_{V'\boxtimes W'}\right)_{G\times H}$$
故不同构的 (V, W) 给出不同构的 $V \boxtimes W$. 计算共轭类数目可知此法穷尽了 $G \times H$ 的所有不可约表示.

3. 齐次 m 次多项式 $\sum_{a+b=m} c_{a,b}x^ay^b$ 在 $\left(\begin{smallmatrix}\epsilon & 0 \\ 0 & \epsilon^{-1}\end{smallmatrix}\right)$ 下变为
$$\sum_{a+b=m} c_{a,b}\epsilon^{a-b}x^ay^b$$

从而不变性导致 $c_{a,b} \neq 0 \implies n \mid a-b$, 这样的项 $x^a y^b$ 总能够写成 $(xy)^k x^{nh}$ 或 $(xy)^k y^{nh}$ 之形; 再考虑 $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ 下的不变性可得 $c_{a,b} = c_{b,a}$. 所以 D_{2n} 的全体整不变量恰好是 $\mathbb{C}[xy, x^n + y^n]$.

4. 运用 [BAIII, p.33] 中对此二维表示的描述: 只要考虑 Q_8 生成元在 $\mathbb{C}^2$ 上之作用

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

下的不变量.

§4.1

1. 事实: $p \nmid a \iff$ 同余式 $ax \equiv 1 \pmod{p}$ 有解.
2. 以下两题似乎须假设 K 是 (交换) 整环并使用 Zorn 引理. 若 $x \notin \mathfrak{m}$ 则理想 xK 不包含于任何极大理想.
3. 略

§4.2

1. 令 $\bar{a}, \bar{b} \in K/pK$ 表示 $a, b \in K$ 在商同态下的像, 则 $p|ab \iff \bar{a}\bar{b} = 0$.
2. 给定理想 $\{0\} \neq I \subsetneq K$, 考虑 $K[X]$ 中由 I 和变元 X 生成的理想 (I, X).
3. 仿照对付 Gauss 整数环的办法验证 K 配上

$$N : x + y\sqrt{-3} \longmapsto x^2 + 3y^2$$

具有带余除法. 为证明子环 $\mathbb{Z}[\sqrt{-3}] = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$ 无唯一分解性质, 仅须证明存在 $a \in \mathbb{Z}[\sqrt{-3}]$ 使得 a 不可约 (即: $d|a \iff a, d$相伴) 但非素元. 一种取法是 $a := 1 + \sqrt{-3}$, 在 $\mathbb{Z}[\sqrt{-3}]$ 中验证

$$a \big| 2(1 - \sqrt{-3}),$$
$$a \nmid 2,$$
$$a \nmid 1 - \sqrt{-3}.$$

欲证明 a 不可约, 仅须留意到 $d|a \implies N(d)|N(a) = 4$, 情况甚少.

4. 在相伴意义下, 素元分三类: (甲) $1+\sqrt{-1}$; (乙) 素数 p 满足 $p \equiv 3 \pmod 4$ 者; (丙) $N(z)=p$ 的任意解, 其中素数 $p \equiv 1 \pmod 4$. 论证略去.

5. 互素的定义见 pp.135–136.

6. 略.

7. 可应用 $(\mathbb{Z}/p\mathbb{Z})^\times$ 是 $p-1$ 阶循环群这一性质.

8. 对于奇素数 p, 在 $\mathbb{Z}[\sqrt{-1}]$ 中计算

$$\begin{aligned}(1+\sqrt{-1})^p &= (1+\sqrt{-1})\left((1+\sqrt{-1})^2\right)^{\frac{p-1}{2}} \\ &= 2^{\frac{p-1}{2}}(1+\sqrt{-1})\sqrt{-1}^{\frac{p-2}{2}},\end{aligned}$$

从而根据上一题在商环 $\mathbb{Z}[\sqrt{-1}]\big/ p\mathbb{Z}[\sqrt{-1}]$ 中导出等式

$$1+(-1)^{\frac{p-1}{2}}\sqrt{-1} \equiv \left(\frac{2}{p}\right)(1+\sqrt{-1})\sqrt{-1}^{\frac{p-1}{2}} \pmod p.$$

借此验证

$$\left(\frac{2}{p}\right) = \begin{cases}(-1)^{\frac{p-1}{4}}, & p \equiv 1 \pmod 4\\ (-1)^{\frac{p+1}{4}}, & p \equiv 3 \pmod 4).\end{cases}$$

并推出所求公式.

9. 为了将多项式等同于多项式函数, 不妨假设 $f(X)$ 的系数在一个无限域 $\Bbbk$ 上; 这不影响结论, 并且总是可行的: 例如可将域 $\Bbbk$ 扩展到一元有理函数域 $\Bbbk(t)$.

若 $f(1)=0$, 则 $f(A)=f(A)f(1)=0$ 故 f 为零函数. 否则 $f(1)=f(1)^2=1$, 并且 $f(A)f(A^{-1})=f(1)=1$ 故 f 在 $\mathrm{GL}(n,\Bbbk)$ 上恒非零. 我们只须在 $\mathrm{GL}(n,\Bbbk)$ 上证明 $\exists m \geq 0,\ f=\det^m$, 因为这蕴涵多项式函数 $\det\cdot(f-\det^m)$ 在 $M_n(\Bbbk)$ 上恒为零, 此处的多项式环是整环故 $f-\det^m=0$.

定义 $E_{s,t}$ 为仅有第 (s,t) 个位置为 1, 其它位置为 0 的 $n\times n$-矩阵. 根据线性代数知群 $\mathrm{GL}(n,\Bbbk)$ 由以下元素生成:

- 对角矩阵 $\mathrm{diag}(x,1,\ldots,1)$, $x\in\Bbbk^\times$;
- 对于 $1\leq s\neq t\leq n$ 和 $\lambda\in\Bbbk$, 矩阵

$$E_{s,t}(\lambda) := 1+\lambda E_{s,t}$$

- 对于 $1 \leq s \neq t \leq n$, 将第 s, t 列对调并变号的矩阵

$$F_{s,t} := \sum_{i \neq s,t} E_{ii} + E_{st} - E_{ts}.$$

依序证明

(i) 题目中的 f 限制在形如 $\mathrm{diag}(x, 1, \ldots, 1)$ 的矩阵上必为 $\mathrm{diag}(x, 1, \ldots, 1) \mapsto x^m$ 的形式, $m \in \mathbb{Z}_{\geq 0}$;

(ii) $F_{s,t}$ 亦可写成诸 $E_{i,j}(\lambda)$ 的积 (利用 p.40 的计算);

(iii) 证明多项式函数 $\lambda \mapsto f(E_{s,t}(\lambda))$ 是常数 1. 一种办法是令

$$A_s(\mu) := \mathrm{diag}(1, \ldots, \underbrace{\mu}_{s}, \ldots, 1), \quad \mu \in \Bbbk^{\times},$$

并作如下观察 ($s \neq t$)

$$A_s(\mu) E_{s,t}(\lambda) A_s(\mu)^{-1} = E_{s,t}(\mu\lambda),$$
$$f(A_s(\mu) E_{s,t}(\lambda) A_s(\mu)^{-1}) = f(E_{s,t}(\lambda)).$$

从此导出在 $\mathrm{GL}(n, \Bbbk)$ 上有 $f = \det^m$.

§4.3

1. 这是标准的内容. 复向量空间 V 连同线性变换 $A : V \to V$ 使得 V 成为 $\mathbb{C}[X]$-模: $f(X) \cdot v = f(A)v$. 将 $\mathbb{C}[X]$-模 V 唯一地分解成形如 $\mathbb{C}[X]/(p(X))$ 的模的直和, 这里可假设 $p(X) = (X - \lambda)^k$, 相应的子模 $V(\lambda) \subset V$ 就是特征值 λ 的根子空间. 进一步可化约到幂零 ($\lambda = 0$) 情形再导出标准型, 见 [BAII, §2.4].

2. 略.

3. 略.

§4.4

1. 仿照第一章处理四元数之法, 容易证明 $x \in \mathbb{H}(n, m)$ 可逆当且仅当 $N(x) \neq 0$. 下面证明若 $p > 2$ 为素数, 而且同余式 $X^2 \equiv 2 \pmod{p}$ 无解, 则 $x \in \mathbb{H}(2, p)$, $N(x) = 0$ 蕴涵 $x = 0$. 如此则按 §4.2 习题 8 可知

$$p \equiv \pm 3 \pmod{8} \implies X^2 \equiv 2 \pmod{p} \text{ 无解}.$$

从而 $\mathbb{H}(2,p)$ 中的非零元皆可逆.

若 $x_0^2 - 2x_1^2 - px_2^2 + 2px_3^2 = 0$ 而 $(x_0, x_1, x_2, x_3) \neq \vec{0}$, 不妨设 x_i 均为整数, 并可进一步假设 $x_0, \ldots, x_3$ 无公因子, 否则提出. 考虑等式 $x_0^2 - 2x_1^2 = p(x_2^2 - 2x_3^2)$. 两边 mod p 并运用 $X^2 \equiv 2 \pmod p$ 无解的条件可得 $x_0, x_1 \in p\mathbb{Z}$. 故等式右边被 p^2 整除, 亦即 $x_2^2 - 2x_3^2 \equiv 0 \pmod p$; 重复同样论证可得 $x_2, x_3 \in p\mathbb{Z}$. 于是 p 是 $x_0, \ldots, x_3$ 的公因数, 矛盾.

2. 见课本提示, 包括共轭运算的定义.

3. 略.

4. 第一部分按

$$\begin{gathered} t(x,y,z) = t((xy)z) - t(x(yz)), \quad (t,x,y)z = ((tx)y)z - (t(xy))z, \\ (tx,y,z) = ((tx)y)z - (tx)(yz), \quad -(t,xy,z) = -(t(xy))z + t((xy)z), \\ (t,x,yz) = (tx)(yz) - t(x(yz)) \end{gathered}$$

来直接计算即可. 对于第二部分, 关键在导出 $(x,y,z) = 0$ 对所有 $x,y,z \in A$ 成立. 设若 $(x,y,z) \in P \cdot 1$ 非零, 第一部分证明的等式导致

$$\forall t \in A, \ (x,y,z)t + (t,x,y)z \in P \cdot 1,$$

因此 A 作为 P-向量空间由 z 和 1 生成. 仅须证明 $\dim_P A \leq 2$ 蕴涵 A 是结合代数即足. 一维情形下 $A \simeq P$; 二维情形下设 $\{1, z\}$ 是 A 在 P 上的基, 那么代数 A 的乘法由常数 $u, v \in P$ 和等式 $zz = uz + v1$ 完全确定, 由此容易证明 $(z,z,z) = 0$, 并且进一步导出结合性.

5. 见课本提示.

6. 利用 Burnside 定理 (p.155) 证明此时 $\forall A, \ \mathrm{tr}(CA) = 0$.

§4.5

略.

§5.1

1. 对任意中间域 L 都有 $[F : P] = [F : L][L : P]$.

2. 一种选择是取 $u := \sqrt{p} + \sqrt{q}$, 并试着以 u^3 和 u 表示 $\sqrt{p}$ 和 $\sqrt{q}$.

3. 先论证分裂域为 $L := \mathbb{Q}(\sqrt[p]{2}, \omega)$, 其中 $\omega \in \mathbb{C}$ 是 p 次本原单位根 (即: $\omega^n = 1 \iff p \mid n$). 然后观察到

   - $[\mathbb{Q}(\omega) : \mathbb{Q}] \mid [L : \mathbb{Q}]$, $\quad [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \mid [L : \mathbb{Q}]$;
   - $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ (原因: ω 是 $\frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1$ 的根, 根据 [BAI, p.171] 这不可约, 因此是 ω 的极小多项式),
   - $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$;
   - $[\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}(\omega)] \leq [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]$.

   由此导出 $[L : \mathbb{Q}] = [L : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = p(p-1)$.

4. 见课本提示.

5. 见课本提示.

§5.2

1. 见课本提示.

2. 仍见课本提示.

3. 先作一个简单的观察: 设 $z \in \mathbb{C}$ 具有极小多项式

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \quad \forall a_i \in \mathbb{Z}.$$

   并假设 (a) n 为偶数, (b) f 无实根, (c) $|z| = 1$. 那么复根共轭蕴涵 $a_0 \in \mathbb{Z}_{\geq 1}$. 上式代入 z, 取复共轭再乘以 z^n 遂给出

$$1 + a_{n-1}z + \cdots + a_0 z^n = 0.$$

   与 $f(z) = 0$ 比较立见 $a_0 = 1$, 而且系数满足对称性 $a_k = a_{n-k}$. 当然, 系数对称性在模 p 后仍成立.

   今假设 Φ_{15} 有不可约因子 f, 且 $\zeta := \exp(\frac{2\pi i}{15})$ 为其根. 由于

$$\Phi_{15} \bmod 2 = (X^4 + X^3 + 1)(X^4 + X + 1) \in \mathbb{F}_2[X] \quad (\text{不可约分解}),$$

   根据 Gauss 引理和 $\mathbb{F}_2[X]$ 的唯一分解性, 可设 f 是首一整系数多项式, 并且

   - 或者 $\deg f = 8 = \deg \Phi_{15}$, 此时 $\Phi_{15} = f$ 不可约;
   - 或者 $f \bmod 2$ 在 $\mathbb{F}_2[X]$ 中等于 $X^4 + X^3 + 1$ 或 $X^4 + X + 1$, 此时 $\deg f = 4$.

将先前观察应用于 f, ζ 可排除第二种情形, 因为在 $\mathbb{F}_2[X]$ 中 X^4+X^3+1 和 X^4+X+1 的系数都不对称.

4. 只消在 $\mathbb{C}[X]$ 里验证. 令 $\zeta := \exp(\frac{2\pi i}{np})$, 则 ζ^n 是 p 次本原单位根, 于是

$$\begin{aligned}\Phi_n\left(X^p\right) &= \prod_{\substack{1\leq b<n \\ (b,n)=1}} \left(X^p - \zeta^{pb}\right) \\ &= \prod_{\substack{1\leq b<n \\ (b,n)=1}} \prod_{0\leq k<p} \left(X - \zeta^{b+nk}\right).\end{aligned}$$

带余除法给出双射

$$\begin{aligned}\{0,\ldots,n-1\}\times\{0,\ldots,p-1\} &\longrightarrow \{0,\ldots,pn-1\} \\ (b,k) &\longmapsto b+nk.\end{aligned}$$

考察 $\{(b,k) : (b,n)=1\}$ 在此双射下的像. 当 $p \mid n$ 时, $a := b+nk$ 满足 $(a,pn) = 1 \iff (a,n)=1 \iff (b,n)=1$, 因此 $\Phi_n(X^p) = \Phi_{pn}(X)$.

若 $p \nmid n$, 我们仍有 $(b+nk,n)=1 \iff (b,n)=1$; 另方面 $(a,n)=1 \wedge (a,pn) \neq 1 \implies p \mid a$. 故

$$\{a = bn+k : (b,n)=1\} = \{a : (a,pn)=1\} \sqcup \{a = ph : (h,n)=1\}.$$

依此整理 $\Phi_n(X^p)$ 为

$$\Phi_n\left(X^p\right) = \prod_{(a,pn)=1}\left(X-\zeta^a\right) \cdot \prod_{(h,n)=1}\left(X-\zeta^{ph}\right) = \Phi_{pn}(X)\Phi_n(X).$$

5. 每个不可约多项式 $f \in \mathbb{F}_p[X]$ 的分裂域都同构于某个 $\mathrm{GF}(p^d)$; 然而 $d \mid p^{d!}$, 故只要 $n \geq d$ 则 f 在 $\mathrm{GF}(p^{n!})$ 上分裂为一次因式.

6. 只需讨论 $(\mathbb{F}_q)^\times$ 中的平方. 因为 $(\mathbb{F}_q)^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$, 仅须在加法群 $\mathbb{Z}/(q-1)\mathbb{Z}$ 中操作: 当 $2 \mid q$ 时 $a \mapsto 2a$ 是 $\mathbb{Z}/(q-1)\mathbb{Z}$ 的自同构; 当 $2 \nmid q$ 时, 它的像是 $2\mathbb{Z}\big/(q-1)\mathbb{Z}$, 亦即 $\ker\left[a \mapsto \frac{q-1}{2}\cdot a\right]$.

7. 又见课本提示.

8. 考虑 $\mathbb{F}_{p^2}$ 的情形, 其中 p 是素数. 它唯一的子域是 $\mathbb{F}_p$, 因而本原元素的数目为 $|\mathbb{F}_{p^2} \smallsetminus \mathbb{F}_p| = p^2 - p$. 根据简单的群论, 乘法群 $\mathbb{F}_{p^2}^\times \simeq \mathbb{Z}/(p^2-1)\mathbb{Z}$ 的生成元数目为

$\phi(p^2-1)$, 这里 $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ 表 Euler 函数. 按定义有

$$\phi(p^2-1) \le (p^2-1) - \frac{p^2-1}{p+1} = p^2-1-(p-1) = p^2-p$$

容易看出 $p>2$ 时不等式严格成立, 故存在非 $\mathbb{F}_{p^2}^\times$ 生成元的本原元素.

9. 我们简要说明 Witt 等式. 为此得假设 §4.5 关于 Lie 代数的一些知识, 以及泛包络代数和自由代数 $A(q)$ 的基本性质. 首先观察到以下泛性质: 对任意 F-代数 B, 线性映射 $f: L(q) \to B$ 如满足

$$f([X,Y]) = f(X)f(Y) - f(Y)f(X), \quad X, Y \in L(q),$$

则存在唯一的 F-代数的同态 φ 使得下图交换

$$\begin{tikzcd} L(q) \arrow[r, hook] \arrow[dr, "f"'] & A(q) \arrow[d, "\varphi"] \\ & B \end{tikzcd}$$

诚然, 唯一的选取由 $\varphi(X_i) = f(X_i)$ 确定 $(i = 1, \ldots, q)$, 而自由性保证 φ 是良定的同态. 此性质表明 $A(q)$ 连同嵌入 $L(q) \to A(q)$ 可以等同于 Lie 代数 $L(q)$ 的泛包络代数 $\mathcal{U}(L(q))$. 因为 $L(q)$ 有一组形如 $b_I := [\ldots[X_{i_1}, X_{i_2}], \ldots]$ 的基, 其中 $I = (i_1, i_2, \ldots)$ (但不易给出 I 的具体取法), 将基的下标 I 任意排序, 著名的 Poincaré–Birkhoff–Witt 定理断言: $A(q)$ 有一组形如 $b_I b_J b_K \cdots$ 的基, 其中 $I \ge J \ge K \ge \cdots$. 由于每个 b_I 都满足于

$$b_I \in L_{|I|}(q) \subset A_{|I|}(q), \quad |I| := i_1 + i_2 + \cdots,$$

故对所有 $m \ge 0$

$$q^m = \dim A_m(q) = \left| \left\{ b_I b_J b_K \cdots : \begin{array}{c} I \ge J \ge K \ge \cdots, \\ |I| + |J| + |K| + \cdots = m \end{array} \right\} \right|$$

从而有生成函数的等式

$$\begin{aligned} \prod_{n=0}^{\infty} (1-X^n)^{-\dim L_n(q)} = \prod_{b_I:\text{基}} \left(1 - X^{|I|}\right)^{-1} = \sum_{m=0}^{\infty} q^m X^m \\ = (1-qX)^{-1}. \end{aligned}$$

两边形式地取对数后展开, 比较系数可得 $\sum_{d|n} d \dim L_d(q) = q^n$. 应用 Möbius 变换

即得 $\dim L_n(q) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right) q^d$.

§5.3

1. 设 $a \in P \smallsetminus \{0\}$. 第一步是证明若 $X^p - a$ 在 $P(\zeta)$ 上或者可约, 或者分裂成一次因子之积. 设 α 是 $X^p - a$ 的根, 取在 $P(\zeta)$ 的某个有限扩张 L 中, 于是 $X^p - a = \prod_{h=0}^{p-1}(X - \alpha\zeta^h)$. 考虑 α 在商群 $L^\times/P(\zeta)^\times$ 中的阶数, 因为 $\alpha^p = a \in P$, 这只能是 $1, p$. 对于 $X^p - a$ 在 $P(\zeta)[X]$ 中的任意首一因式 Q, 其常数项可写作 ζ 的某个幂次乘上 $(-\alpha)^{\deg Q}$, 于是 $\alpha^{\deg Q} \in P(\zeta)^\times$ 蕴涵 $\deg Q = 1$ 或 p, 后者对应到 $X^p - a$ 在 $P(\zeta)$ 上不可约的情形.

   以下设 $X^p - a$ 在 $P(\zeta)$ 上分裂, 亦即 $\alpha \in P(\zeta)^\times$. 容易看出 $P(\zeta)/P$ 是 Galois 扩张, 其 Galois 群 G 作用在根集 $\left\{\alpha\zeta^h : 0 \le h < p\right\}$ 上. 已知 G 透过对 ζ 的作用嵌入为 $(\mathbb{Z}/p\mathbb{Z})^\times$ 的子群 (见 [BAI, p.187]), 因此是循环群; 选定生成元 $\tau \in G$, 以及由 $\tau(\zeta) = \zeta^g$ 所刻画的 $g \in (\mathbb{Z}/p\mathbb{Z})^\times$.

   等式 $\tau(\alpha) = \alpha\zeta^{k(\alpha)}$ 唯一确定了 $k(\alpha) \in \mathbb{Z}/p\mathbb{Z}$, 今后取定它在 $\mathbb{Z}$ 中的代表元. 若 $X^p - a$ 在 P 中无根, 则对每个 α 皆有 $p \nmid k(\alpha)$, 在此假设下计算 G-作用的稳定化子群:

   $$\tau^r(\alpha) = \alpha\zeta^{k(\alpha)(1+g+\cdots+g^{r-1})}, \quad r \in \mathbb{Z}.$$

   于是

   $$\tau^r(\alpha) = \alpha \iff k(\alpha)\sum_{i=0}^{r-1} g^i \equiv 0 \pmod{p} \iff \sum_{i=0}^{r-1} g^i \equiv 0 \pmod{p}.$$

   最后一式无关 α 的选择. 由此可见根集的 G-轨长恒定, 故整除根的数目 p. 由于 $\tau(\alpha) \neq \alpha$, 故 G 在根集上的作用传递. 于是 $X^p - a$ 在 P 上也不可约 (直接论证或参考 [BAI, §5.4 定理 2]). 这就导致如下矛盾: $X^p - a$ 是 α 的极小多项式, 从而

   $$p = [P(\alpha) : P] \mid [P(\zeta) : P] \le \left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1.$$

   综上, 若 $X^p - a$ 在 $P(\zeta)$ 上可约, 则它在 P 中有根.

2. 容易验证这些多项式都不可约 (对四次情形应用 Eisenstein 判准). 可以利用 §5.4 定理 1 及其推论: 对于无重根不可约多项式 f, 其 Galois 群 $G_f \subset S_n$ 满足 $G_f \le A_n$ 当且仅当判别式 $D(f) \in (F^\times)^2$ (判别式已在 [BAI, §6.2] 提及), 而且 $\mathbb{Q}\left(\sqrt{D(f)}\right)$ 对应到 $G_f \cap A_n$. 特例: 三次多项式 $X^3 + aX + b$ 的判别式为 $-4a^3 - 27b^2$. 顺带留意到 G_f 在根集 $\{r_1, \ldots, r_n\} \xrightarrow{1:1} \{1, \ldots, n\}$ 上的作用传递.

关于四次方程的准备: 对于多项式 $f = X^4 - a_1X^3 + a_2X^2 - a_3X + a_4 \in \mathbb{Q}[X]$, 设其根为 $r_1, r_2, r_3, r_4 \in \mathbb{C}$, 并定义

$$\begin{aligned} t_1 &:= r_1r_2 + r_3r_4, \\ t_2 &:= r_1r_3 + r_2r_4, \\ t_3 &:= r_1r_4 + r_2r_3. \end{aligned}$$

证明 $g := (X - t_1)(X - t_2)(X - t_3)$ 可写作 $g = X^3 - b_1X^2 + b_2X - b_3$, 其中

$$\begin{aligned} b_1 &= a_2, \\ b_2 &= a_1a_3 - 4a_4, \\ b_3 &= a_1^2a_4 + a_3^2 - 4a_2a_4. \end{aligned}$$

这是四次方程的预解式, 详见 N. Jacobson, *Basic Algebra I. 2nd ed.* New York: W. H. Freeman and Company (1985), 第 261 页. 我们将用到以下性质: 设 $D(f) \notin (\mathbb{Q}^\times)^2$ 而 $L_g := \mathbb{Q}(t_1, t_2, t_3)$ 为 $\mathbb{Q}$ 的二次扩张, 那么 $L_g = \mathbb{Q}\left(\sqrt{D(f)}\right)$, 从下面的计算中也可看出这点.

(a) 计算判别式可知 G 包含于 A_3, 传递性蕴涵 $G \simeq A_3$. 此题或书后答案有笔误.

(b) 计算判别式知 G 不包含于 A_3, 而 S_3 中不包含于 A_3 的传递子群只有 S_3 自身.

(c) 同上.

(d) 计算可知判别式为 $2048 = 2^{11}$, 预解式为 $g = X^3 - 4X^2 - 8X + 32 = (X - 4)(X^2 - 8)$. 先说明对四次方程总有 $4 \mid |G|$, 故 $G \subset S_4$ 可能的阶数为 4, 8, 12, 24.
   - 因 A_4 是 S_4 唯一的 12 阶子群, 考虑判别式知 $|G| \neq 12$;
   - 假若 $G = S_4$, 则 $(123) \in G$ 在 L_g 上诱导 3-循环 $t_1 \mapsto t_3 \mapsto t_2 \mapsto t_1$, 与 $[L_g : \mathbb{Q}] = 2$ 矛盾;
   - 若 $|G| = 8$ 则 G 是 S_4 的 Sylow 2-子群, 此时必共轭于 $D_4 \subset S_4$ (二面体群), 然而这蕴涵

   $$G \cap A_4 = V := \{1, (12)(34), (13)(24), (14)(23)\}$$

   是传递的, 从而 $f = X^4 + 4X^2 + 2$ 在 $L_g = \mathbb{Q}(\sqrt{2})$ 上不可约, 这点极易否证;
   - 若 $|G| = 4$ 则传递性蕴涵 $G \simeq \mathbb{Z}/4\mathbb{Z}$, 此即答案.

(e) 照搬之前方法, 计算判别式为 $2052 = 2^2 3^3 19$, 预解式为 $g = X^3 - 21X - 36 = (X + 3)(X^2 - 3X - 12)$, 于是 $L_g = \mathbb{Q}\left(\sqrt{3 \cdot 19}\right)$. 说明只可能有 $G \simeq \mathbb{Z}/4\mathbb{Z}$ 或 $G \simeq D_4$ 两种情形. 假若 $G \simeq \mathbb{Z}/4\mathbb{Z}$, 那么 $G \cap A_4$ 为二阶群, 此时 $f = X^4 + 3X^3 - 3X + 3$ 在 L_g 上分解成 $f = f_1f_2$, 其中 $\deg f_1 = \deg f_2 = 2$ 并可假设为首一. 自同

构 $\tau \in \mathrm{Gal}(L_g/\mathbb{Q})$, $\tau \neq \mathrm{id}$ 逐系数地作用在 $L_g[X]$ 上, 给出环自同构. 由唯一分解立得

- 或者 $\tau(f_1) = f_1, \tau(f_2) = f_2$, 这时 $f_1, f_2 \in \mathbb{Q}[X]$ 故矛盾;
- 或者 $\tau(f_1) = f_2$. 考察 f_1 的常数项 c 可知 $3 = c\tau(c)$; 应用一些简单的代数数论 (略) 可知

$$c = \frac{a + b\sqrt{3 \cdot 19}}{2}, \quad a, b \in \mathbb{Z},\ a \equiv b \pmod 2.$$

  故 $a^2 - 57b^2 = 2^2 3$, 导出 3 是模 19 的二次剩余, 然而 $\left(\frac{3}{19}\right)$ 等于

$$3^{\frac{19-1}{2}} = (3^3)^{2+1} \equiv 8^2 8 \equiv 7 \cdot 8 \equiv -1 \pmod{19}$$

  矛盾.

综上, $G \simeq D_4$. 详尽的解说见 Keith Conrad, Galois groups of cubics and quartics (not in characteristic 2).

§5.4

1. 正规基的概念见课本 p.197. 容易看出多项式 X^3+X+1 在 $\mathbb{F}_2$ 上无根, 故不可约. 验证课本提示中的 $\theta+1$ 确给出 $\mathbb{F}_8 = \mathbb{F}_2[\theta]\big/(\theta^3+\theta+1)$ 的正规基: 计算它在自 Frobenius 自同构下的轨道为 $\theta+1$, θ^2+1 和 $\theta^4+1 = \theta^2+\theta+1$; 由于 $\mathbb{F}_8 = \mathbb{F}_2 \oplus \mathbb{F}_2\theta \oplus \mathbb{F}_2\theta^2$, 这是容易计算的.

2. 先注意到 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 确实是 Galois 扩张: 它是 $(X^2-2)(X^2-3)$ 的分裂域. 依序验证下述性质.

   - 论证 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, 因此其 Galois 群是四阶群.
   - Galois 群的任意元素 σ 必映 $\sqrt{2}$ 为 $\pm\sqrt{2}$, 映 $\sqrt{3}$ 为 $\pm\sqrt{3}$, 这种四阶群必然同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 其中正好元素对应到 $\frac{\sigma\sqrt{2}}{\sqrt{2}}$ 和 $\frac{\sigma\sqrt{3}}{\sqrt{3}}$ 四种可能的正负号组合.
   - 说明 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ 是 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 的一组基.
   - 验证 $1+\sqrt{2}+\sqrt{3}+\sqrt{6}$ 在 Galois 群作用下的像给出正规基.

   根据 Galois 群的显式描述, 最后一步不外是简单的 4×4 矩阵消元.

§5.5

1. 可. 显然 $x=0$ 非解, 原方程可化为 $(x^3+x^{-3})+2(x^2+x^{-2})-5(x+x^{-1})+9=0$. 进一步将之化为 $y:=x+x^{-1}$ 的三次方程来求解.

2. 将题目中的 α_i 写作
$$\alpha_i=\zeta^i u+\zeta^{-i}v, \quad 0\le i\le 4,$$
其中的复数 u,v 满足 $u^5v^5=a^5$ 而 $u^5+v^5=2b$. 用这些性质直接在 $\mathbb{Q}[x]$ 中展开乘积来验证
$$\prod_{i=0}^{4}(x-\alpha_i)=x^5-5ax^3+5a^2x-2b.$$
因此 $\alpha_0,\ldots,\alpha_4$ 确实给出原方程的根 (含重数). 这可谓是 Cardano 方法对五次方程的一种推广, 参见 B. Spearman, K. Williamson, *Characterization of solvable quintics* x^5+ax+b, Amer. Math. Monthly 101 (1994), no. 10, 986–992 的讨论 (http://www.jstor.org/stable/2975165).

3. 见课本提示.

4. 见课本提示. 关于 Lagrange 预解式的讨论亦见聂灵沼, 丁石孙《代数学引论》第二版 (北京: 高等教育出版社, 2000 年), §8.4.

§5.6

略.