1. Let G be a set with an operation $\cdot$ such that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

for any $a, b, c \in G$. Then if G satisfies that

(1) there exists $e \in G$, such that $a \cdot e = a$ for any $a \in G$;

(2) for any $a \in G$, there exists $b \in G$ such that $a \cdot b = e$.

Then $(G, \cdot, e)$ is a group.

解答 我们需要证明: (i) 对任意 $a \in G$, 我们有 $e \cdot a = a \cdot e = a$. (ii) 对任意 $a \in G$, 存在 $b \in G$, 使得 $a \cdot b = b \cdot a = e$.

对任意 $a \in G$, 根据 (1), 存在 $b, c \in G$ 使得 $a \cdot b = b \cdot c = e$. 现考虑 $b \cdot a = b \cdot a \cdot e = b \cdot a \cdot (b \cdot c) = b \cdot (a \cdot b) \cdot c = (b \cdot e) \cdot c = b \cdot c = e$. 所以 $a \cdot b = b \cdot a = e$, 即 (i) 成立.

对上述 $a, b \in G$, $e \cdot a = (a \cdot b) \cdot a = a \cdot (b \cdot a) = a \cdot e = a$. 所以 $a \cdot e = e \cdot a = a$, 即 (ii) 成立. □

2. Let $G := \{(a_{ij})_{n\times n} | a_{ij} \in \mathbb{Z} \text{ and } |(a_{ij})_{n\times n}| = 1 \text{ or } -1\}$. Prove that G is a group respect to the matrix multiplication.

解答 假设 $A = (a_{ij})_{n\times n}, B = (b_{ij})_{n\times b} \in G$. 根据矩阵的乘法, 我们有 $|AB| = |A||B|$, 故 $|AB| = 1$ 或 -1 且 AB 中的 (i,j) 项为 $\sum_{k=1}^{n} a_{ik}b_{kj} \in \mathbb{Z}$, 所以 G 对乘法封闭. 又因为单位阵 I 显然在 G 中, 且 $IA = AI = A$. 假设 A 的代数余子式为 A^*, 因为 A^* 中的 (i,j) 项都是 A 中的项的多项式, 所以 A^* 中的项仍为整数. 因为 $A^{-1} = (\det A)^{-1} A^*$ 且 $\det A = \pm 1$, $\det A^{-1} = \pm 1$, 所以 $A^{-1} \in G$. 显然 $AA^{-1} = A^{-1}A = I$, 故 G 是群. □

3. Let J be a fixed $n \times n$ matrix over $\mathbb{R}$ with $|J| \neq 0$. Prove that

$$G := \{A \mid A \in \mathbb{R}^{n\times n}, AJA^T = J\}$$

is a group respect to the matrix multiplication.

解答 $G \subset \mathsf{GL}_n(\mathbb{R})$, 我们只需证明对任意 $A, B \in G$, 都有 $AB \in G$ 且 $A^{-1} \in G$. 因为 $ABJ(AB)^T = ABJB^TA^T = A(BJB^T)A^T = AJA^T = J$, 所以 $AB \in G$. 因为 $AJA^T = J$, 所以 $J = A^{-1}J(A^T)^{-1} = A^{-1}J(A^{-1})^T$, 所以 $A^{-1} \in G$. □

4. Let M be an arbitrary set, and $P(M)$ be the set consisting of all the subsets of M. Prove that $P(M)$ is a group respect to the operation

$$A \cdot B = (A - B) \bigcup (B - A).$$

解答 令 $E = \emptyset$, 对任意 $A \in P(M)$, 我们有 $E \cdot A = A \cdot E = A$, 且 $A \cdot A = E$. 我们需要证明结合性. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. 注意到可定义双射 $\chi : P(M) \to \mathrm{Hom}(M, \mathbb{Z}_2)$. 注意到 $\chi_{A\cdot B} = \chi_A + \chi_B$. 从而 $\chi((A \cdot B) \cdot C) = \chi_{A\cdot B} + \chi_C = \chi_A + \chi_B + \chi_C = \chi_A + \chi_{B\cdot C} = \chi_{A\cdot(B\cdot C)} = \chi(A \cdot (B \cdot C))$. 所以 $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. □

5. Let G be a group with operation $\cdot$, and S be a nonempty set. Let $M(S, G)$ be the set consisting of all the map $f : S \to G$ with the operation

$$f * g : S \to G,$$

$$s \mapsto f(s) \cdot g(s)$$

Prove that $M(S, G)$ is a group respect to above operation $*$.

解答 对任意 $s \in S$, 我们有 $(f*g)*h(s) = (f*g)(s)\cdot h(s) = (f(s)\cdot g(s))\cdot h(s) = f(s)\cdot(g(s)\cdot h(s)) = f(s)\cdot(g*h)(s) = f*(g*h)(s)$, 即 $(f*g)*h = f*(g*h)$. 令 $e : S \to G$ 定义为对任意 $s \in$, $e(s) = 1_G$. 那么对任意 $s \in S$, $e * f(s) = e(s)\cdot f(s) = f(s) = f(s)\cdot e(s) = f * e(s)$, 所以 $e * f = f * e = f$. 对于 $f \in M(S, G)$, 对每个 $s \in S$, 定义 $f^{-1}(s) = f(s)^{-1}$, 那么 $(f * f^{-1})(s) = f(s)\cdot f^{-1}(s) = 1_G = e(s) = f^{-1}(s)\cdot f(s) = (f^{-1} * f)(s)$, 所以 $f * f^{-1} = f^{-1} * f = e$. □

6. Prove that: for any abelian group G, we have

$$\circ(ab) \leqslant \circ(a) \circ (b)$$

for any $a, b \in G$. On the same time, point out there exists non-abelian group such that above equality is not valid.

解答 假设 $\circ(a) = m, \circ(b) = n$, 即 $a^m = b^n = e$, 那么又因为 G 是 Abel 群, $(ab)^{mn} = (a^m)^n(b^n)^m = 1$. 所以 $\circ(ab) \leqslant mn$.

令

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

我们发现 $a^4 = b^3$ 是单位阵. 那么 ab 的阶是无限的, 要想有限阶, 则可以在模 n 的世界中操作 (只需要 $n \geqslant 13$ 即可). □

7. Prove that the group $(\mathbb{Q}, 0, +)$ is not isomorphic to $(\mathbb{Q}^* := \mathbb{Q} - \{0\}, 1, x)$.

解答 第一个群没有二阶元, 因为 $2x = 0$ 推出 $x = 0$; 第二个群存在二阶元, $(-1)^2 = 1$, 故两个群不同构. □

8. Prove that there exists no simple group G of order $|G| = 56$.

解答 根据 Sylow 定理, Sylow-7 子群的个数模 7 余 1, 且是 8 的因子, 所以有 1 个或 8 个. 如果有 1 个, 那么这个 Sylow-7 子群是正规子群. 如果有 8 个, 那么 7 阶元有 $48 = (7-1)*8$ 个, 还剩 $56 - 48 = 8$ 个非 7 阶元. 所以 Sylow-2 子群只有一个, 故为正规子群. □

9. Prove that any group G of order $|G| = 35$ is cyclic, namely $G = (a)$ for some $a \in G$.

解答 根据 Sylow 定理, Sylow-7 子群只有 1 个 N. 而 Sylow 5 子群也只有一个 H. H 共轭作用在 N 上, 得到一个群作用 $\mathbb{Z}_5 \simeq H \to \mathrm{Aut}(N) \simeq U(\mathbb{Z}_7) = \mathbb{Z}_6$. 所以只有平凡作用. 所以对任意 $a \in H, b \in N$, 我们有 $ab = ba$. 令 x 是 H 的生成元, y 是 N 的生成元, 那么 xy 的阶是 35, 所以 $G = (xy)$. □

10. Let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, and $U(\mathbb{Z}_n)$ be the group of all units (invertible elements in $\mathbb{Z}_n$). Prove that

$$\bar{m} \in U(\mathbb{Z}_n) \iff (m, n) = 1.$$

解答 根据 Bezout 定理, 如果 $(m, n) = 1$, 那么存在 $mx + ny = 1$, 所以模 n 后得到 $\bar{m}\bar{x} = \bar{1}$, 即 $\bar{m} \in U(\mathbb{Z}_n)$.

如果 $m \in U(\mathbb{Z}_n)$, 那么存在 $\bar{x} \in \mathbb{Z}_n$, $\bar{m}x = \bar{1}$, 所以存在 $y \in \mathbb{Z}$, 使得 $mx + ny = 1$. 那么 $(m, n)|1$, 即 $(m, n) = 1$. □

11. Let $G = (a)$ be a cyclic group of order n. Prove that its group of isomorphisms $\mathrm{Aut}(G) \simeq U(\mathbb{Z}_n)$. In particular, when $n = p$ is a prime number, $\mathrm{Aut}(G)$ is also cyclic.

解答 由于 $G=(a)$, 任何 $f\in \mathrm{Aut}(G)$ 由 $f(a)$ 决定, 所以 $f(a)$ 是 G 中的 n 阶元. 但是 $x\in\mathbb{Z}_n$ 的阶恰是 $n/(n,x)$. 所以 $\mathrm{Aut}(G)\simeq U(\mathbb{Z}_n)$.

有限域的乘法子群是循环群. 设 $U(\mathbb{Z}_p)$ 中最大阶为 n, 不妨设 $\circ(x)=n$. 由于 $U(\mathbb{Z}_p)$ 是交换群, 所以该群中每个元素的阶整除 n. 如若不然, 存在一个非平凡元素的阶和 n 互素, $\circ(y)=m$, 且 $(m,n)=1$. 所以 xy 的阶为 mn, 矛盾. 又因为在域中 $x^n=1$ 的根最多 n 个, 所以 $n\leqslant |U(\mathbb{Z}_p)|\leqslant n$. 所以存在 $p-1$ 阶元. $\square$

12. Let R be a (noncommutative) ring, and $1-ab$ is invertible. Prove that $1-ba$ is also invertible.

解答 设 $(1-ab)c=1$, 那么 $(1+bca)(1-ba)=1-ba+bca-bcaba=1-ba+bc(1-ab)a=1$. $\square$

13. Let R be a ring, then a non-zero element x is called by a nilpotent element if $x^n=0$ for some $n\in\mathbb{Z}^+$. Prove:

(1) If x is nilpotent, then $1-x$ is invertible.

(2) The ring $\mathbb{Z}_m:=\mathbb{Z}/m\mathbb{Z}$ has a nilpotent element if and only if m can be divisible by p^2 for some $p\in\mathbb{Z}^+$.

解答

(1) 如果 $x^n=0$, 那么 $(1-x)(1+x+x^2+\cdots+x^{n-1})=1-x^n=1$. 所以 $1-x$ 是可逆的.

(2) 如果 $m=p^2n$, 那么 $p\bar{n}\neq 0$, 但是 $(p\bar{n})^2=p\bar{2}n\cdot n=0$. 反之, 不妨假设 $x^2=0,x\neq 0$. 令 $h=m/(m,x)\neq 1$, 则 $m=h^2\cdot\frac{(m^2,x^2)}{m}$.

$\square$

14. Let $m,n\in\mathbb{Z}$ be positive. Prove that the great common divisor $(m,n)\in\mathbb{Z}$ equals to $(m,n)\in\mathbb{Z}[i]$.

解答 假设在 $\mathbb{Z}$ 中, 我们有 $(m,n)=a, m=am', n=an'$. 于是 $\mathbb{Z}[i]$ 中, $(m,n)=a(m',n')$. 但是存在 $x,y\in\mathbb{Z}$ 使得 $m'x+n'y=1$. 如果 $\mathbb{Z}[i]$ 中有素数 p 满足 $p|(m',n')$, 那么 $p|m'x+n'y$, 即 $p|1$, 矛盾. $\square$

15. Let R be a ring. Prove that $f(x)\in R[x]$ is a zero divisor if and only if $r\cdot f(x)=0$ for some $r\neq 0\in R$.

解答 使用反证法. 假设 g 是最小次数的非零多项式使得 $fg=0$. 令

$$f(x)=a_0+a_1x+\cdots+a_kx^k+\cdots+a_nx^n$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m$$

假设 k 是使得 $a_kg(x)\neq 0$ 的最大值, 如果不存在, 则对任意 $0\leqslant i\leqslant m$, 都有 $b_if(x)=0$, 矛盾. 因为 $f(x)g(x)=0$, 则 $a_kb_m=0$, 从而 $\deg(a_kg(x))<\deg(g(x))$. 我们有 $f(x)(a_kg(x))=0$, 矛盾. $\square$

16. Prove that $\mathbb{C}[x,y]/(x^2+y^2-1)$ is an Euclidean ring.

解答 令 $u=x+iy, v=x-iy$, 那么 $R:=\mathbb{C}[x,y]/(x^2+y^2-1)=\mathbb{C}[u,v]/(uv-1)\simeq\mathbb{C}[u,u^{-1}]$. 因此 R 中每个非零元素都可以唯一的写为 $u^mf(u)$ 的形式, 其中 $f(u)\in\mathbb{C}[u], f(0)\neq 0, m\in\mathbb{Z}$. 现在定义 $u^mf(u)\mapsto\deg(f(u)):R^*\to\mathbb{N}$ 的欧式映射 δ. 对于任意 $u^mf(u), u^ng(u)$, 因为 $\mathbb{C}[u]$ 是欧式环, 存在 $q(u),r(u)\in\mathbb{C}[u]$ 使得

$$f(u)=g(u)q(u)+r(u),\quad u^mf(u)=u^ng(u)\cdot u^{m-n}q(u)+u^mr(u)$$

那么 $\delta(u^m r(u)) \leqslant \deg(r(u)) < \delta(u^n g(u))$ 或 $r(u) = 0$. 所以 $\mathbb{C}[x,y]/(x^2+y^2-1)$ 是 Euclidean 环. $\square$

17. Prove that $\mathbb{R}[x,y]/(x^2+y^2-1)$ is not an UFD.

解答 我们已经证明了 $\mathbb{C}[x,y]/(x^2+y^2-1)$ 是 ED, 从而是 UFD. 或者说 $R = \mathbb{C}[u,u^{-1}]$ 是 UFD. 考虑 $x \cdot x = (1-y)\cdot(1+y)$. 在 $\mathbb{C}[u,u^{-1}]$ 中,

$$x = \frac{1}{2u}(u+i)(u-i)$$

$$1-y = \frac{i}{2u}(u-i)^2$$

$$1+y = \frac{-i}{2u}(u+i)^2$$

所以 $x \cdot x = (1-y)\cdot(1+y)$ 是两个不可约分解. $\square$

18. Prove that $\mathbb{C}[x,y]/(x^2-y^3)$ is not an UFD.

解答 由于 $\mathbb{C}[x,y]$ 是 UFD, 因为 x^2-y^3 是不可约元, 所以是素元, 从而 $R \coloneqq \mathbb{C}[x,y]/(x^2-y^3)$ 是整环. 如果赋予 x 次数 3, y 次数 2, 那么 R 是分次环, 且 x, y 是不可约元. 因为 $x\cdot x = y \cdot y \cdot y$ 是两个不同的不可约分解. 所以 R 不是 UFD. $\square$

19. Prove that $R[x]$ is an UFD, provided R is so.

解答 记 $f(x) = \sum_{i=0}^n a_i x^i$, 令 $d(f) = (a_0, \cdots, a_n)$. 于是 $f(x) = d(f) f_0(x)$. 将 $f_0(x)$ 写成 $p_1(x)\cdots p_t(x)$ 的形式, 其中 $p_i(x)$ 是不能写成两个次数更低的多项式的乘积. 由高斯引理知这些 $p_i(x)$ 是本原多项式, 于是不可约; 因为 R 是 UFD, $d(f) = a_1 \cdots a_s$ 为 R 中的唯一分解. 我们得到一个不可约分解:

$$f(x) = a_1 \cdots a_s p_1(x) \cdots p_t(x).$$

假设 $f(x) = b_1 \cdots b_k q_1(x) \cdots q_l(x)$ 是另一个不可约分解, 于是 $q(x) = q_1(x)\cdots q_l(x)$ 和 $p(x) = p_1(x)\cdots p_t(x)$ 是本原多项式. 于是 $a_1 \cdots a_s \cdot d(p(x)) \backsim d(f) \backsim b_1 \cdots b_k \cdot d(q(x))$. 因为 R 是 UFD, $s = k$, 可设 $a_i \backsim b_i$. 因此存在 $u \in U(R)$ 使得 $p(x) = uq(x)$.

考虑 $K = Q(R)$ 是 R 的分式域, 则 $p_i(x), q_j(x)$ 也是不可约的. 因为 $K[x]$ 是 UFD, 从而 $t = l$, 可设 $p_i(x) = v_i q_i(x), v_i \in K$. 但是 $p_i(x)$ 和 $q_i(x)$ 是本原多项式, 所以 $p_i(x) \backsim q_i(x) (1 \leqslant i \leqslant t)$. $\square$

20. Let $F \subset E$ and $E \subset K$ be two finite algebraic extensions. Prove that $F \subset K$ is a finite algebraic extension.

解答 因为 $[K:F] = [K:E]\cdot[E:F]$, E/F 和 K/E 是有限代数扩张, 从而 $[K:F] < \infty$. $\square$

21. Prove that the isomorphisms of $\mathbb{Q}$ and $\mathbb{R}$ are both trivial (only identities).

解答 设 $f \in \mathrm{Aut}(\mathbb{Q})$, $f(1) = 1, f(0) = 0$, 对于 $n \in \mathbb{N}$, $f(n) = \underbrace{f(1) + \cdots + f(1)}_{n个} = n$, $f(-n) = f(0-n) = f(0) - f(n) = -n$. 对于 $\frac{m}{n} \in \mathbb{Q}$, $\underbrace{f(\frac{m}{n}) + \cdots + f(\frac{m}{n})}_{n个} = f(n \cdot \frac{m}{n}) = f(m) = m$, 从而 $f(\frac{m}{n}) = \frac{m}{n}$. 所以 $f = \mathrm{id}_{\mathbb{Q}}$.

假设 $g \in \mathrm{Aut}(\mathbb{R})$, 同理可得 $g|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. 对每个 $x > 0$, $g(x) = g((\sqrt{x})^2) = g(\sqrt{x})^2 > 0$, 因此如果 $a > b$, 我们有 $g(a) = g(b) + g(a-b) > g(b)$. 由 Dedekind 分割, 每个无理数 α 和 $g(\alpha)$ 给出有理数相同的分割, 从而 $\alpha = g(\alpha)$. $\square$

22. Let $\mathbb{R} \subset K$ be a finite algebraic extension with $[K : \mathbb{R}] = 2$. Prove that K is isomorphic to $\mathbb{C}$.

解答 假设 $\alpha \in K \setminus \mathbb{R}$, α 在 $\mathbb{R}$ 上的极小多项式为 $f(x) \in \mathbb{R}[x]$. 由于 $1 < \deg f(x) \leqslant [K : \mathbb{R}]$, 所以 $\deg f(x) = 2$. 不妨设 $f(x) = x^2 + bx + c$. 因为 $f(x)$ 在 $\mathbb{R}[x]$ 上不可约, 所以 $\Delta = b^2 - 4c < 0$. 从而 $y = \frac{2x+b}{\sqrt{4c-b^2}} \in K$ 满足 $y^2 + 1 = 0$. 所以 $K \supset \mathbb{R}[y] \supsetneq \mathbb{R}$, 从而 $K = \mathbb{R}[y] \simeq \mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$. □

23. Let $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{5}] \subset \mathbb{R}$ be subfields. Prove that $\mathbb{Q}[\sqrt{2}]$ is not isomorphic to $\mathbb{Q}[\sqrt{5}]$.

解答 假设 $f : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$ 是同构, 设 $f(\sqrt{2}) = a + b\sqrt{5}, a, b \in \mathbb{Q}$. 那么 $f(\sqrt{2})^2 = f(2) = 2$, 所以 $(a + b\sqrt{5})^2 = 2$. 展开得 $a^2 + 5b^2 + 2ab\sqrt{5} = 2$, 所以 $ab = 0$. 如果 $a = 0$, 得 $5b^2 = 2$; 如果 $b = 0$, 得 $a^2 = 2$. 均得到矛盾. □

24. Let F be a finite field, and $F^* := F - \{0\}$. Prove that $(F^*, \times, 1)$ is a cyclic group.

解答 记 $G = F^*$. G 是一个 Abel 群. 设 G 中元素阶最大的元素为 a, 且 $\circ(a) = n$. 首先证明对任意 $b \in G$, $b^n = 1$. 如果不然, 存在 $b \in G \setminus \{1\}$, b 的阶为 m 且 $(m, n) = 1$. 那么 $\circ(ab) = mn$, 矛盾. 但是在域 F 中 $x^n = 1$ 的解最多 n 个, 所以 $n = \circ(a) \leqslant |G| \leqslant n$. 所以 $n = |G|$, 从而 $G = (a)$ 是循环群. □

25. Construct a non-separable polynomial.

解答 固定一个特征为 p 的完全域 F. 令 $K = F(t)$. 那么 $t \in K \setminus K^p$. 记 $L = K[\alpha]$ 是 f 的分裂域, 其中 $\alpha^p = t$. 考虑多项式 $f(x) = x^p - t$. 这是一个那么 $f(x) \in K[x]$ 是不可约多项式. 否则 $f(x) = g(x)h(x)$. 它在 $L[x]$ 中就变成 $(x - \alpha)^p = g(x)h(x)$, 故不妨设 $g(x) = (x - \alpha)^{n_1}, h(x) = (x - \alpha)^{n_2}$, 从而常数项 $u = \alpha^{n_1}, v = \alpha^{n_2} \in K$. 因为 $(n_1, n_2) = 1$, 存在 $a, b \in \mathbb{Z}$, 使得 $an_1 + bn_2 = 1$. 从而 $u^a v^b = \alpha \in K$,$t = \alpha^p \in K^p$, 矛盾. □

26. Prove that one can construct regular 17-gons using straight-edge and compass.

解答 因为 $\cos \frac{2\pi}{17}$ 是包含在 $\mathbb{Q}$ 的某个二次根塔里面. 所以可被尺规作图. □

27. Prove that one can not construct regular 7-gons using straight-edge and compass.

解答 考虑 7 次单位根 ω, 则 ω 的极小多项式是 $x^6 + x^5 + \cdots + x + 1 = 0$. 所以 $[\mathbb{Q}[\omega] : \mathbb{Q}] = 6$ 不是 2 的幂次, 所以不可以被尺规作图. □

28. Let $K \subset L$ be a Galois extension, and $K \subset E \subset L$. Prove that E/K is Galois if and only if $\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$ is a normal subgroup.

解答 如果 E/K 是 Galois 的, 那么所有的 L 的 K 自同构 σ 都有 $\sigma(E) = E$. 考虑 $h \in \mathrm{Gal}(L/E), g \in \mathrm{Gal}(L/K)$, 那么对于任意 $x \in E$, 我们有 $g^{-1}(x) \in E, hg^{-1}(x) = g^{-1}(x)$, 且 $ghg^{-1}(x) = gg^{-1}(x) = x$, 所以 $ghg^{-1} \in \mathrm{Gal}(L/E)$.

如果 L 的 K 自同构 σ 使得存在 $x \in E$, 但是 $\sigma(x) \notin E$. 存在 $h \in \mathrm{Gal}(L/E)$ 使得 $y := h(\sigma(x)) \neq \sigma(x)$. 那么 $\sigma^{-1}h\sigma(x) = \sigma^{-1}(y) \neq \sigma^{-1}(\sigma(x)) = x$. 所以 $\sigma^{-1}h\sigma \notin \mathrm{Gal}(L/E)$. □

29. Prove that $f(x) = x^n - 1 \in \mathbb{Q}[x]$ can be solved by radicals.

解答 $x^n - 1 \in \mathbb{Q}[x]$ 的一个分裂域为 $L = \mathbb{Q}[\omega]$, 他的全部根的集合

$$U_n = \{\omega^k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}\}$$

那么 $\mathrm{Gal}(L/\mathbb{Q})$ 作用在 U_n 上得到单同态 $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Aut}(U_n) \simeq U(\mathbb{Z}_n)$. 因为这个群是交换群, 所以可解. 从而 $f(x)$ 可根式解. □

30. Construct a polynomial $f(x) \in \mathbb{Q}[x]$, which cannot be solved by radicals.

解答 取 $p=5$ 使用爱森斯坦判别法可知 $f(x)=x^5-80x+5\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上不可约, 利用单调性可知 $f(x)$ 恰有两个非实数根, 故 $G_f=S_5$ 不可解. $\square$

31. Prove (by a direct computation) that $\mathbb{Q}=(\mathbb{Q}[\sqrt{2},\sqrt{11}])^G$ where $G=\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{11}]/QQ)$ is the Galois group.

解答 注意到 $\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{11}]/\mathbb{Q})$ 同构于 $\mathbb{Z}_2\times\mathbb{Z}_2$, 由 $\sigma_1:\sqrt{2}\mapsto-\sqrt{2},\quad\sqrt{11}\mapsto\sqrt{11}$ 和 $\sigma_2:\sqrt{2}\mapsto\sqrt{2},\quad\sqrt{11}\mapsto-\sqrt{11}$ 生成. 假设 $x=a+b\sqrt{2}+c\sqrt{11}+\sqrt{22}\in(\mathbb{Q}[\sqrt{2},\sqrt{11}])^G$, 那么 $\sigma_1(x)=a-b\sqrt{2}+c\sqrt{11}-d\sqrt{22}$, 所以 $b=d=0$, $\sigma_2(x)=a-c\sqrt{11}$, 所以 $c=0$. 从而 $x=a\in\mathbb{Q}$. $\square$