Lecture Notes On Abstract Algebra (Week 16)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 30 (Dec 19, 2023): Galois Theorem

1.1 Kummer Extensions

Let us have a close look at a special single radical extension.

Proposition 1.1. *Let n be a positive integer prime to the characteristic of F. Assume that F contains all n-th roots of unity and α is a root of $x^n - a$ with $a \in F$. Then $F(\alpha)/F$ is a cyclic extension of degree d and $\alpha^d \in F$, where d is a divisor of n.*

Proof. Since n is prime to the characteristic of F and F contains all n-th roots of unity, then F contains a primitive n-th root of unity ζ. Consequently all roots of $x^n - a$ are $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$. Hence $F(\alpha)/F$ is Galois. Let $\sigma \in G = \mathrm{Gal}\,(F(\alpha)/F)$. Then $\sigma(\alpha) = \alpha\zeta^k$ for some $0 \le k \le n-1$ and σ is determined by a unique k. Set $\sigma_k \in G$ via

$$\sigma_k(\alpha) = \alpha\zeta^k.$$

Then $G = \{\sigma_k \mid k \in I\}$, where I is a subset of $\{0, 1, 2, \ldots, n-1\}$. We obtain an embedding from the Galois group G to the additive group $\mathbb{Z}/n\mathbb{Z}$ as

$$\begin{aligned} \nu : G = \mathrm{Gal}\,(F(\alpha)/F) &\hookrightarrow \mathbb{Z}/n\mathbb{Z} \\ \sigma_k &\mapsto \overline{k} = k \bmod n. \end{aligned}$$

Since $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n, G must be cyclic of order d, a divisor of n. That is, $F(\alpha)/F$ is cyclic of degree d.

Write $n = dm$. Notice that $\langle \overline{m} \rangle$ is the only subgroup of order d of the additive group $\mathbb{Z}/n\mathbb{Z}$. Hence $I = \{k \mid 0 \le k \le n-1, d \mid m\}$ and

$$G = \mathrm{Gal}\,(F(\alpha)/F) = \{\sigma_{0,}\sigma_m, \sigma_{2m}, \ldots, \sigma_{(d-1)m}\}.$$

Set

$$\varphi(x) = \prod_{i=0}^{d-1} (x - \sigma_{im}(\alpha)) = \prod_{i=0}^{d-1} \left(x - \alpha\,(\zeta^m)^i\right).$$

Notice that ζ^m is a primitive d-th root of unity. We have $\varphi(x) = x^d - \alpha^d$. On the other hand, $\varphi(x) \in F[x]$, since the coefficients of $\varphi(x)$ is fixed by G (i.e, $\sigma_{im}(\varphi(x)) = \varphi(x)$). It follows from Theorem 1.2 in Lecture 24 that $\alpha^d \in F$. □

An extension as in Proposition 1.1 is called a Kummer Extension. More precisely, if F contains all n-th roots of unity and n is prime to char(F), then an extension of the form $F(\sqrt[n]{a})$ is called a **Kummer extension** over F. By Proposition 1.1, a Kummer extension is always cyclic and a single radical extension is a Kummer extension if the base field contains enough roots of unity.

Problem Let p be a prime which is prime to char(F). Assume F contains all p-th root of unity and K/F is a Galois extension of degree p. Show that K/F is a Kummer extension.

1.2 Galois Theorem

Recall a result on single radical extensions.

Let n be a positive integer prime to the characteristic of F. Assume that F contains a primitive n-th root of unity and α is a root of $x^n - a$ with $a \in F$. Then $F(\alpha)/F$ is cyclic of degree d with $d \mid n$, and $\alpha^d \in F$.

Hence a single radical extension is a Kummer extension if the base field contains enough roots of unity.

Theorem 1.1 (Galois). *If a polynomial with coefficients in a field F of characteristic zero is solvable by radicals, then its Galois group over F is a solvable group.*

Proof. Let $f(x) \in F[x]$ be solvable by radicals. Then the splitting field L of $f(x)$ is contained in some field $F_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_1^{m_1} \in F$ and $\alpha_i^{m_i} \in F_{i-1} = F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for some $m_i \in \mathbb{Z}$ and for each $i = 2, 3, \ldots, n$. Let $\widetilde{F_n}$ be a normal closure of F_n. Then $\widetilde{F_n}$ is a compositum of conjugates of F_n. Notice that each F_i is achieved by adjoining a series of radicals successively, i.e. F_i/F_0 is a radical extension. It follows that $\widetilde{F_n}$ is also achieved by adjoining a series of radicals, hence a radical extension over F_0. Thus, we may replace F_n by its normal closure $\widetilde{F_n}$, if necessary. For simplicity, we may assume that F_n/F is normal, hence Galois, from the beginning.

Let $\ell = [m_1, m_2, \ldots, m_n]$ be the least common multiple of $m_1, m_2, \ldots, m_n$ and let ζ_ℓ be a primitive ℓ-th root of unity. Set $K_0 = F(\zeta_\ell)$, $K_i = F_i K_0 = F_i(\zeta_\ell), 1 \le i \le n$. Then $K_i = K_{i-1}(\alpha_i)$ is a Kummer extension over K_{i-1}.

Since F_n/F and K_0/F are Galois, so their compositum $K_n = F_n K_0$ is also a Galois extension over F. Let

$$G = \mathrm{Gal}(K_n/F) \text{ and } G_i = \mathrm{Gal}(K_n/K_i),\ i = 0, 1, \ldots, n.$$

Since $K_i = K_{i-1}(\alpha_i)$ is a Kummer extension over K_{i-1} and K_{i-1} contains all m_i-th root of unity, the extension K_i/K_{i-1} is cyclic by Proposition 1.1. Then $G_i \lhd G_{i-1}$ and $G_{i-1}/G_i \cong \mathrm{Gal}(K_i/K_{i-1})$ is cyclic, by the Fundamental Theorem of Galois Theory.

$$\begin{tikzcd}
& K_n = F_nK_0 \arrow[d, dash] \\
F_n \arrow[ur, dash] \arrow[d, dash] & K_{n-1} = F_{n-1}K_0 \arrow[d, dash] \\
F_{n-1} \arrow[d, dash] & \vdots \arrow[d, dash] \\
\vdots \arrow[d, dash] & K_1 = F_1K_0 \arrow[d, dash] \\
F_1 \arrow[d, dash] & K_0 = F(\zeta_\ell) \\
F = F_0 \arrow[ur, dash] &
\end{tikzcd}
\qquad
\begin{tikzcd}
K_n \arrow[d, dash] \arrow[d, bend left, dash, "G_i"] \arrow[dd, bend right=60, dash, "G_{i-1}"'] \\
K_i \arrow[d, dash] \arrow[d, bend left, dash, "\text{Galois}"] \\
K_{i-1}
\end{tikzcd}
\qquad
\begin{tikzcd}
K_n \arrow[d, dash] \arrow[dd, bend right=60, dash, "G"'] \\
L \arrow[d, dash] \arrow[d, bend left, dash, "G_f"] \\
F
\end{tikzcd}$$

Similarly, K_0/F is a cyclotomic extension, hence $G_0 \lhd G$ and G/G_0 is abelian. Setting $G_{-1} = G$, we have a normal group series

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 \lhd G_{-1} = G$$

for G such that all G_{i-1}/G_i are abelian, $i = 0, 1, 2 \cdots, n$. Thus, G is solvable.

Now the Galois group of $f(x)$, $\mathrm{Gal}(L/F)$, is a quotient group of $G = \mathrm{Gal}(K_n/F)$, hence is solvable. □

Remark 1.1. Galois also proved that the converse of Theorem 1.1 is true (see the following exercise). Actually,

let F be a field of characteristic zero, then a polynomial $f(x) \in F[x]$ is solvable by radicals if and only if its Galois group over F is solvable.

Exercises

1. The following procedures provide an approach to prove the converse of Theorem 1.1.

   (1) Let E/F be a finite Galois extension and K/F is algebraic. Then EK/K is also Galois and $\mathrm{Gal}(EK/K)$ can be embedded in $\mathrm{Gal}(E/F)$ as a subgroup.

   (2) If E/F is a cyclic extension of degree n and F contains all n-th roots of unity, then $E = F(\alpha)$ for some $\alpha \in E$ with $\alpha^n \in F$. In particular, E/F is a Kummer extension.

   (3) Let E be a splitting field of $f(x)$ over F and the Galois group G_f of $f(x)$ over F is solvable of order n. Take ζ_n to be a primitive n-th root of unity over F. Then there exist intermediate fields F_i of $E(\zeta_n)/F(\zeta_n)$ such that

   $$F_1 = F(\zeta_n) \subseteq F_2 \subseteq \cdots \subseteq F_m = E(\zeta_n)$$

   and F_i/F_{i-1} is cyclic of degree p_i, where p_i is a prime divisor of n, $2 \le i \le m$. Consequently, E is contained in some radical extension of F.

   (4) If the Galois group of $f(x)$ over F is solvable, then $f(x)$ is solvable by radical.

2. Let $\alpha = \sqrt[3]{1 + \sqrt{2}}$ with minimal polynomial $m(x)$ over $\mathbb{Q}$.

   (1) Compute $m(x)$.

   (2) Show that $m(x)$ is solvable by radicals.

2 Lecture 31 (Dec 21, 2023): Insolvability of the Quintic Polynomials

2.1 Insolvability of the Quintic Polynomials

Inverse Galois Problem For any finite group G, is there a Galois extension F of $\mathbb{Q}$ satisfying $\mathrm{Gal}(F/\mathbb{Q}) = G$?

In this section we will show that the problem is true for S_p, where p is a prime. In particular, we show that there exists a quintic polynomial which is not solvable by radicals. This implies that a general quintic polynomial is not solvable by radicals.

Basic Fact For the full symmetric group S_n, we have

$$\begin{aligned} S_n &= \langle (i_1 i_2 \cdots i_r) \mid 1 \leq i_1, i_2, \ldots, i_r \leq n \rangle, \\ &= \langle (i_1 i_2) \mid 1 \leq i_1 < i_2 \leq n \rangle, \\ &= \langle (1\, i) \mid 1 < i \leq n \rangle, \\ &= \langle (i, i+1) \mid 1 \leq i \leq n-1 \rangle. \end{aligned}$$

Since

$$\begin{aligned} &(i_1 i_2 \cdots i_r) = (i_1 i_r) \cdots (i_1 i_4)(i_1 i_3)(i_1 i_2), \\ &(i_1 i_2 \cdots i_r) = (1 i_r) \cdots (1 i_4)(1 i_3)(1 i_2) \quad \text{if} \quad i_1 = 1 \quad \text{and} \\ &(i_1 i_2 \cdots i_r) = (1\, i_2 \cdots i_r i_1)(1\, i_1) = (1\, i_1)(1 i_r) \cdots (1 i_3)(1 i_2)(1\, i_1) \quad \text{if} \quad i_1, i_2, \ldots, i_r \neq 1, \\ &\quad (i, i+1) = (1i)(1, i+1)(1i), \\ &\quad (1, i+1) = (1\, i)(i, i+1)(1\, i). \end{aligned}$$

Lemma 2.1. *The symmetric group S_n is generated by (12) and $(12 \cdots n)$.*

Proof. The result follows from the fact that

$$S_n = \langle (i, i+1) \mid 1 \leq i \leq n-1 \rangle$$

and

$$(12 \cdots n)^{i-1} (12) (12 \cdots n)^{1-i} = (i, i+1)$$

for $i = 1, 2, \ldots, n-1$. □

We can also prove that $S_n = \langle (12), (12 i_3 i_4 \cdots i_n) \rangle$, where $\{i_3, i_4, \ldots, i_n\} = \{3, 4, \ldots, n\}$.

Lemma 2.2. *Let p be a prime number and let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree p. Suppose that $f(x)$ is irreducible over $\mathbb{Q}$ and has exact $p-2$ real roots. Then the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p.*

Proof. If α is a root of $f(x)$ then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ since $f(x)$ is irreducible and $\deg f = p$. Thus, if L is a splitting field for $f(x)$ over $\mathbb{Q}$, then $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$ by the Tower Law (Transitivity of Degree of Field Extensions) and therefore $[L : \mathbb{Q}]$ is divisible by p. But $[L : \mathbb{Q}]$ is the order of the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ of $f(x)$, and therefore $p \mid |G|$. It follows from Sylow Theorem that G must contain at least one element of order p. Moreover an element of G is determined by its action on the roots of $f(x)$. Thus an element of G is of order p if and only if it cyclically permutes the roots of $f(x)$.

The irreducibility of $f(x)$ ensures that $f(x)$ has distinct roots. Let α_1 and α_2 be the two roots of $f(x)$ that are not real. Then α_1 and α_2 are complex conjugates of one another, since $f(x)$ has real coefficients.

We have already seen that G contains an element of order p which cyclically permutes the roots of $f(x)$. On taking an appropriate power of this element, we obtain an element σ of G that cyclically permutes the roots of $f(x)$ and sends α_1 to α_2. We label the real roots $\alpha_3, \alpha_4, \ldots, \alpha_p$ of $f(x)$ so that $\alpha_j = \sigma(\alpha_{j-1})$ for $j = 3, 4, \ldots, p$. Then $\sigma(\alpha_p) = \alpha_1$. Now complex conjugation restricts to a $\mathbb{Q}$-automorphism τ of L that interchanges α_1 and α_2 but fixes α_j for $j > 2$. We get a group embedding

$$\begin{aligned} G &\hookrightarrow S_p, \\ \sigma &\mapsto (12\cdots p), \\ \tau &\mapsto (12). \end{aligned}$$

It follows from Lemma 2.1 that the above embedding is surjective and thus G is isomorphic to S_p. □

Now consider the quintic polynomial $f(x) = x^5 - 6x + 3$. Eisenstein's Criterion can be used to show that $f(x)$ is irreducible over $\mathbb{Q}$. Now $f(-2) = -17, f(0) = 3, f(1) = -2$ and $f(2) = 23$. The Intermediate Value Theorem ensures that $f(x)$ has at least 3 distinct real roots. If $f(x)$ had at least 4 distinct real roots then Rolle's Theorem would ensure that the number of distinct real roots of f' and f'' would be at least 3 and 2 respectively (do you remember what Rolle's Theorem says?). But zero is the only root of f'' since $f''(x) = 20x^3$. Therefore $f(x)$ must have exactly 3 distinct real roots. It follows from Lemma 2.2 that the Galois group of $f(x)$ is isomorphic to the symmetric group S_5. This group is not solvable. Galois Theorem ensures that the polynomial $x^5 - 6x + 3$ is not solvable by radicals over $\mathbb{Q}$.

The above example demonstrates that there **cannot** exist any general formula for obtaining the roots of a quintic polynomial from its coefficients in a finite number of steps involving only addition, subtraction, multiplication, division and the extraction of n-th roots. Because if such a general formula were to exist then every quintic polynomial with rational coefficients would be solvable by radicals. So we obtain

Theorem 2.1 (Abel-Ruffini, 1824). *A general quintic polynomial over $\mathbb{Q}$ is not solvable by radicals.*

Corollary 2.1. *A general polynomial of degree n over $\mathbb{Q}$ is not solvable by radicals, when $n \geq 5$. (当$n \geq 5$时, n次方程不能根式求解)*

Proof. Let $f(x) = x^{n-5}(x^5 - 6x + 3)$. Then $\deg f = n$. The polynomial $f(x)$ and $x^5 - 6x + 3$ possess a same splitting field. Hence the Galois group of $f(x)$ is isomorphic to S_5, an unsolvable group. Therefore $f(x)$ is not solvable by radicals by Galois Theorem. □

Remark 2.1. Paolo Ruffini made an incomplete proof of the above Theorem 2.1 in 1799, and Niels Henrik Abel provided a proof in 1824, which contains complicated computation and some gaps.

Galois appreciates beautiful structures. He said: "Jump above calculations, group the operations, classify them according to their complexities rather than their appearance; this, I believe, is the mission of future mathematicians; this is the road I'm embarking in this work." (跳出计算, 群化运算, 按照它们的复杂性而不是表象来分类; 我相信, 这是未来数学的任务; 这也正是我的工作所揭示出来的道路.)

Exercises

1. Let p be a prime integer. Show that $S_p = \langle (i_1 i_2), (j_1 j_2 \cdots j_p) \rangle$, where $1 \leq i_1 < i_2 \leq p$ and $(j_1 j_2 \cdots j_p)$ is a p-cycle.

2. Show that the Galois group of $x^5 - 20x + 16$ over $\mathbb{Q}$ is S_5.

3. Show that the Galois group of $x^5 + 20x + 16$ over $\mathbb{Q}$ is A_5.

4. Show that the equation $x^5 - 4x + 2 = 0$ is not solvable by radicals over $\mathbb{Q}$.

5. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n > 2$ that has $n-2$ real roots and exactly one pair of complex conjugate roots. Prove that the Galois group of $f(x)$ over $\mathbb{Q}$ is not a simple group.

6. Identify a complex number $a + bi$ with the point (a, b) in the Euclidean plane $\mathbb{R}^2$. A complex number is constructible using straightedge and compasses if the corresponding point is constructible using straightedge and compasses. For given n complex numbers $z_1, z_2, \ldots, z_n$, set $F = \mathbb{Q}(z_1, z_2, \ldots, z_n, \overline{z}_1, \overline{z}_2, \ldots, \overline{z}_n)$. Show that a complex number z is constructible from $\{0, 1, z_1, z_2, \cdots, z_n\}$ by using straightedge and compasses if and only if z is contained in a Galois extension E/F such that $|\mathrm{Gal}(E/F)| = 2^m$ for some integer $m \geq 0$.

7. Show that a regular n-sided polygon is constructible using straightedge and compasses if and only if $n = 2^s p_1 p_2 \cdots p_t$, where $s \geq 0$ and $p_1, p_2, \ldots, p_t$ are distinct Fermat primes (a Fermat prime is a prime number that is of the form $2^k + 1$ for some integer k).

8. Show that a regular 17-sided polygon is constructible using straightedge and compasses.

9. Show that the Galois group of $f(x) = x^5 - x - 1$ is S_5.

   (Van Der Waerden cites in his famous book *Modern Algebra* the polynomial $f(x) = x^5 - x - 1$. The Galois group of $f(x)$ modulo 2 is cyclic of order 6, because $f(x)$ modulo 2 factors into polynomials of orders 2 and 3: $f(x) \equiv (x^2+x+1)(x^3+x^2+1) (\mathrm{mod}\ 2)$. $f(x)$ modulo 3 has no linear or quadratic factor, and hence is irreducible. Thus its modulo 3 Galois group contains an element of order 5. It is known that a Galois group modulo a prime is isomorphic to a subgroup of the Galois group over the rationals. A permutation group on 5 objects with elements of orders 6 and 5 must be the symmetric group S_5, which is therefore the Galois group of $f(x)$. This is one of the simplest examples of a non-solvable quintic polynomial.)

10. (Van Der Waerden) Construct a polynomial $f \in \mathbb{Z}[x]$ of degree $n > 3$ as follows.

    (a) Choose f_1 of degree n which is irreducible modulo 2;

    (b) Choose f_2 which can be factored modulo 3 as a linear factor and an irreducible factor of degree $n-1$;

    (c) Choose f_3 which factors modulo 5 as a quadratic and one or two factors of odd degree (all irreducible modulo 5);

    (d) Choose $f(x)$ such that $f \equiv f_1 (\mathrm{mod}\ 2), f \equiv f_2 (\mathrm{mod}\ 3), f \equiv f_3 (\mathrm{mod}\ 5)$.

    Then the Galois group $\mathrm{Gal}(f(x)/\mathbb{Q})$ is transitive and contains an $n-1$ cycle and a cycle of order 2. This implies that the Galois group $\mathrm{Gal}(f(x)/\mathbb{Q})$ is isomorphic to S_n.

11. Let $x_1, x_2, \ldots, x_n$ be indeterminates over a field F and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the elementary symmetric functions of the x_i's. Show that $[F(x_1, x_2, \ldots, x_n) : F(\sigma_1, \sigma_2, \ldots, \sigma_n)] = n!$.

2.2 Quiz 5

1. (4分) 构造 25 元有限域 $\mathbb{F}_{25}$, 并指出所有本原元.

2. (8分) 设 $F = \mathbb{Q}(\alpha, i)$, 其中 $\alpha = \sqrt[3]{2}$, $i = \sqrt{-1}$. 对 $F/\mathbb{Q}$ 的每个中间域 M, 求一个 $\alpha \in F$ 使得 $M = \mathbb{Q}(\alpha)$, 并指出在 $\mathbb{Q}$ 上为正规扩张的所有非平凡中间域.

3. (8分) 设 $\alpha = \sqrt{2+\sqrt{2}}$, $\beta = \sqrt{2-\sqrt{2}}$, $m(x)$ 为 α 在 $\mathbb{Q}$ 上的极小多项式.

(1) 求 $m(x)$.

(2) 证明 $\beta \in \mathbb{Q}(\alpha)$ 且 $\mathbb{Q}(\alpha)$ 为 $m(x)$ 的分裂域.

(3) 求 $m(x)$ 在 $\mathbb{Q}$ 上的 Galois 群.

Homework Exercise 37, 39 on page 318-319.

3 Practice Problems

3.1 Problems

1. 完成以下问题.

   (1) 有限生成模的商模是有限生成的吗? 若是, 请证明; 若不是, 请举出反例.

   (2) 证明 $\mathbb{Q}(\sqrt{2},\sqrt{5})=\mathbb{Q}(\sqrt{2}+\sqrt{5})$.

   (3) 举一个域的有限扩张的例子, 使得该扩张含有无限多个中间域.

   (4) 叙述尺规三等分角问题, 并简要描述该问题的解决思路.

   (5) 构造元素个数为125的有限域 $\mathbb{F}_{125}$.

   (6) 是否存在这样的交换 3-群(即阶为 3 的方幂的阿贝尔群) G, 使得 G 恰有 9 个 3 阶元? 若有, 刻画该群的结构; 若没有, 说明理由.

2. 设R为整环但不是域, 证明: 多项式环$R[x]$不是主理想整环.

3. 对环 R 中的元素 a, 若有正整数 n 使得 $a^n=0$, 则称 a 为幂零元. 求剩余类环 $R=\mathbb{Z}/45\mathbb{Z}$中的所有零因子, 幂零元和理想, 并指出其中的素理想.

4. 设 R 是定义域为实数域 $\mathbb{R}$ 的(实)函数的集合. 按照通常的函数加法和乘积运算, R 成为一个含幺交换环. 对 $f(x)\in R$, 定义
$$D_f=\{a\in\mathbb{R}\mid f(a+b)=f(b),\ \forall b\in\mathbb{R}\}.$$

   (1) 证明: D_f有一个自然的$\mathbb{Z}$-模结构.

   (2) 设 $R'=\{f(x)\in R\mid \mathbb{Z}\subseteq D_f\}$. 证明: R'是 R 的子环且自然成为一个 $\mathbb{R}$-模. 试问: R' 是整环吗? 为什么?

5. 设 K 为多项式 $f(x)=x^4-x^3+x^2-1$ 在 $\mathbb{Q}$ 上的分裂域, $G=\mathrm{Gal}(K/F)$.

   (1) 求 G 的大小和结构.

   (2) 指出 $K/\mathbb{Q}$ 的所有非平凡的中间域以及它们在 $\mathbb{Q}$ 上的扩张次数.

6. 设 $f(x)=x^4+ax^2+b$ 为 $\mathbb{Q}$ 上的不可约多项式, $d=a^2-4b$, K 为 $f(x)$ 在 $\mathbb{Q}$上的分裂域.

   (1) 证明: d 不是 $\mathbb{Q}$ 中的平方元, 即不存在 $\delta\in\mathbb{Q}$ 使得 $d=\delta^2$;

   (2) 设 α 为 $f(x)$ 的一个根, 证明 $K=\mathbb{Q}(\alpha,\sqrt{b})$, 并推出 $[K:\mathbb{Q}]=4$ 或 8;

   (3) 设 bd 为 $\mathbb{Q}$ 中的平方元, 证明: $\mathrm{Gal}(K/\mathbb{Q})$ 是 4 阶循环群.

3.2 Answers

1. (1) YES. Let M be an R-module generated by $m_1, \ldots, m_n$, then the quotient module $\overline{M}$ is generated by $\overline{m}_1, \ldots, \overline{m}_n$.

   (2) Clearly $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \supseteq \mathbb{Q}(\sqrt{2}+\sqrt{5})$ and $[\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}] = 4$. On the other hand, $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

   (3) Let $F = \mathbb{F}_p(x, y)$ be the rational function field in two variable and $K = \mathbb{F}_p(x^p, y^p)$. Then F/K is a field extension of degree p^2 with infinitely many nontrivial intermediate subfields $F_n = K(x + y^{np+1})(n \geq 1)$.

   (4) The problem "trisecting the angle" states that it is impossible to trisect an arbitrary angle by using straightedge and compasses alone. This problem was solved by showing that $\frac{\pi}{3}$ radians can not be trisected by using straightedge and compasses alone.

   Actually, assume $\frac{\pi}{3}$ could be trisected by using straightedge and compasses alone. Then $a = \cos\frac{\pi}{9}$ is constructible and $[\mathbb{Q}(a) : \mathbb{Q}]$ is a power of 2. Notice $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. On setting $\theta = \frac{\pi}{9}$ we deduce that $4a^3 - 3a = \frac{1}{2}$ or $8a^3 - 6a - 1 = 0$. Thus $a = \cos\frac{\pi}{9}$ is a root to the polynomial $f(x) = 8x^3 - 6x - 1$, which is irreducible by checking the possible rational roots. This implies that $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, a contradiction.

   (5) Since the polynomial $m(x) = x^3 + x + 1$ has no root in $\mathbb{F}_5$, hence irreducible over $\mathbb{F}_5$. Thus $\mathbb{F}_5/(x^3 + x + 1)$ is a finite field with 5^3 elements. We can construct $\mathbb{F}_{125} = \mathbb{F}_5/(x^3 + x + 1)$.

   (6) NO. Let G be an abelian 3-group that can be decomposed into the direct sum of n cyclic 3-groups. Then there are exactly $3^n - 1$ elements of order 3 in G. Now $3^n - 1 = 9$ has no integer solutions. It follows that there is no abelian 3-group with exactly 9 elements of order 3.

2. Let a be a nonzero element in R, not invertible. Then the ideal (a, x) is not principle. Otherwise, there exists some $f(x) \in R[x]$ such that $(a, x) = (f(x))$. It follows that

$$a = f(x)g(x), x = f(x)h(x)$$

   for some $g(x), h(x) \in R[x]$. Since R is a domain, we can see from $a = f(x)g(x)$ that $\deg a = \deg f(x) + \deg g(x) = 0$. Then $\deg f(x) = 0$, that is, $f(x) \in R$ and $f(x) = f(0) \neq 0$. But $f(0)h(0) = 0$ and then $h(0) = 0$. We have $h(x) = x\varphi(x)$ for some $\varphi(x) \in R[x]$. Thus $f(x)\varphi(x) = 1$, yielding $f(x)$ is a unit in $R[x]$. Hence $(a, x) = (1) = R$ and there exist $u(x), v(x) \in R[x]$ such that

$$au(x) + xv(x) = 1.$$

   Then $au(0) = 1$, which implies that a is invertible, a contradiction. Therefore (a, x) is not principle and $R[x]$ is not principle.

3. The zero divisors are $\overline{3x}$ and $\overline{5y}$ for $0 \leq x < 15, 1 < y < 9$. The nilpotent elements are $\overline{0}, \overline{15}, \overline{30}$. The ideals are $(\overline{0}), (\overline{1}), (\overline{3}), (\overline{5}), (\overline{9}), (\overline{15})$, among which $(\overline{3}), (\overline{5})$ are prime ideals .

4. (1) Obviously D_f is an abelian group, hence a $\mathbb{Z}$-module.

   (2) The set R' composed of those real function with period 1. It is closed under addition and multiplication. Hence R' is a subring of R. But R' is not an integral domain. Actually, let $f(x) = \sin(\pi x)$ and $g(x)$ be the function given by $g(x) = 1$ if $x \in \mathbb{Z}$ and $g(x) = 0$ if $x \notin \mathbb{Z}$. Then $f, g \in R'$, nonzero, but $fg = 0$ in R'.

5. (1) Notice that $f(x) = (x-1)(x^3+x+1)$ and the discriminant of $G(x) = x^3+x+1$ is $D(g) = -31 < 0$. Then $|G| = 6$ and $G \cong S_3$.

   (2) Since $G \cong S_3$, G has three subgroups of order 2 and one group of order 3. It follows from Galois theory that there are three intermediate extensions of degree 3 and one intermediate extension of degree 2 over $\mathbb{Q}$.

6. (1) Notice that $g(x) = x^2+ax+b$ must be irreducible, since otherwise $f(x)$ would factorize, hence $d = a^2-4b$ is not a square in $\mathbb{Q}$.

   (2) Taking δ to be a square root of d (so $\delta = \sqrt{a^2-4b} \notin \mathbb{Q}$), we find that the roots of $g(x)$ are $\frac{-a\pm\delta}{2} \notin \mathbb{Q}$ and the roots of $f(x)$ are $\pm\sqrt{\frac{-a\pm\delta}{2}}$. WLOG, we set

$$\alpha^2 = \frac{-a+\delta}{2}, \ \beta^2 = \frac{-a-\delta}{2}.$$

   Then $(\alpha\beta)^2 = b$ and $K = \mathbb{Q}(\alpha,\beta)$. Hence $K = \mathbb{Q}(\alpha, \sqrt{b})$. Since $\deg f(x) = 4$, we have $4 \mid [K:\mathbb{Q}]$. Since

$$K = \mathbb{Q}\left(\sqrt{b}, \sqrt{a^2-4b}, \sqrt{\frac{-a+\sqrt{a^2-4b}}{2}}\right)$$

   is obtained by at most 3 successive quadratic extensions, we have $[K:\mathbb{Q}] \mid 8$. It follows $|G| = 4$ or 8.

   (3) Notice $bd = (\alpha\beta\delta)^2$. If bd is a square in $\mathbb{Q}$, then $\alpha\beta\delta = c \in \mathbb{Q}$ and hence $\beta = \frac{c}{\alpha\delta} \in \mathbb{Q}(\alpha)$. Since $\delta = a + 2\alpha^2 \in \mathbb{Q}(\alpha)$, we have $K = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$ and $|G| = [K:\mathbb{Q}] = 4$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ be give by $\sigma(\alpha) = \beta$. Then $\sigma(\alpha^2) = \beta^2$, yielding $\sigma(\delta) = -\delta$. And

$$\sigma(\beta) = \sigma\left(\frac{c}{\alpha\delta}\right) = -\frac{c}{\beta\delta} = -\alpha.$$

   So $\sigma^2(\alpha) = -\alpha$ and $\sigma^4(\alpha) = \alpha$. This shows that $\sigma \in G$ is an element of order 4. Consequently $G \cong \mathbb{Z}/4\mathbb{Z}$ is cyclic of order 4.