中国科学院大学
试 题 专 用 纸

开课编号：210002H
课程名称：代数学 I
任课教师：李文威

时间: 2015 年 1 月 6 日 13:30-15:10
总分: 100 分

1. **(15 points)** Let E be the splitting field of $P(X) = X^3 - X + 1 \in \mathbb{Q}[X]$; we may assume $E \subset \mathbb{C}$. Determine the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.

   ✎ *Solution*. We present one possible approach below.

   (i) $P(X)$ is irreducible over $\mathbb{Q}$: this is equivalent to the assertion that P has no roots in $\mathbb{Q}$. By elementary algebra, it suffices to check that ± 1 are not roots.
   (ii) $P(X)$ has exactly one real root — this can be done by calculus. Details omitted.
   (iii) We may embed $\mathrm{Gal}(E/\mathbb{Q})$ into $\mathfrak{S}_3$ by its action on the three roots in E. Since $P(X)$ is irreducible, $\mathrm{Gal}(E/\mathbb{Q})$ acts transitively; the complex conjugation permutes the roots of P in $E \subset \mathbb{C}$, therefore gives rise to a transposition in $\mathrm{Gal}(E/\mathbb{Q})$. Hence $\mathrm{Gal}(E/\mathbb{Q}) = \mathfrak{S}_3$.

   Alternatively, one many also argue by considering the discriminant of $P(X)$, etc.

2. **(15 points)** Show that for every $n \geq 1$, there exists a field embedding

   $$\iota : \mathbb{Q}(X_1, \ldots, X_n) \hookrightarrow \mathbb{C}$$

   over $\mathbb{Q}$, where $\mathbb{Q}(X_1, \ldots, X_n)$ stands for the field of rational functions in the variables $X_1, \ldots, X_n$.

   ✎ *Solution*. Using the facts (i) if E/F is an algebraic extension of infinite fields, then $|E| = |F|$; (ii) $|\mathbb{C}| > |\mathbb{Q}|$, one constructs a sequence of complex numbers $\alpha_1, \alpha_2, \ldots$ without nontrivial polynomial relations over $\mathbb{Q}$. The construction goes recursively as follows.

   (a) Choose any transcendental number α_1.
   (b) Assume that $n \in \mathbb{Z}_{\geq 1}$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ have been chosen so that for every $P \in \mathbb{Q}[X_1, \ldots, X_n]$, we have $P(\alpha_1, \ldots, \alpha_n) \neq 0$ whenever $P \neq 0$. In other words, there is no nontrivial polynomial relation among $\alpha_1, \ldots, \alpha_n$. Now choose $\alpha_{n+1} \in \mathbb{C}$ that is not algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. This is possible since $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is countable whereas $\mathbb{C}$ is not.
   (c) We contend that for any $P \in \mathbb{Q}[X_1, \ldots, X_{n+1}]$, $P(\alpha_1, \ldots, \alpha_{n+1}) = 0$ implies $P = 0$. Indeed, assume $P \neq 0$ and let $Q(X_{n+1}) := P(\alpha_1, \ldots, \alpha_n, X_{n+1})$, $Q \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)[X_{n+1}]$. If $Q = 0$ there would be some polynomial relations among $\alpha_1, \ldots, \alpha_n$ (to see this, regard P as a nonzero element of $\mathbb{Q}[X_1, \ldots, X_n][X_{n+1}]$ and look at its coefficients in the ring $\mathbb{Q}[X_1, \ldots, X_n]$), which is impossible. However $Q(\alpha_{n+1}) = 0$ is also impossible by the previous step. Thus $P = 0$.

   Given n, putting $\iota(P(X_1, \ldots, X_n)) = P(\alpha_1, \ldots, \alpha_n)$ for all $P \in \mathbb{Q}(X_1, \ldots, X_n)$ defines the required embedding.

3. **(20 points)** Let R be a ring with unit and let $I \subset R$ be a two-sided ideal whose elements are all nilpotent. Establish the *lifting of idempotents* from R/I to R by the following instructions.

(a) Let $\bar{a} \in R/I$ be an idempotent, i.e. $\bar{a}^2 = \bar{a}$. Suppose that $a \in R$, $a \mapsto \bar{a}$ under the quotient homomorphism $R \to R/I$, and set $b = 1 - a$. Show that $ab = ba \in I$.

(b) For a, b as above and $m \in \mathbb{Z}_{\geq 1}$, put

$$e = \sum_{0 \leq k \leq m} \binom{2m}{k} a^k b^{2m-k},$$
$$f = \sum_{m < k \leq 2m} \binom{2m}{k} a^k b^{2m-k}$$

where $\binom{u}{v} := \frac{u!}{v!(u-v)!}$. Show that $e + f = 1$, $ef = 0$ whenever m is sufficiently large. *Hint*: take $m \gg 0$ so that $(ab)^m = 0$.

(c) Under the assumption $m \gg 0$, deduce that $f^2 = f$ (i.e. $f \in R$ is an idempotent) and f has image $\bar{a}$.

✎ *Solution*. We have $ab = a - a^2 = ba$, which lies in I since $\bar{a} = \bar{a}^2$. The equation $e + f = 1$ follows from the binomial identity. Since b (resp. a) appears with powers $\geq m$ in the expression of e (resp. that of f) and $ab = ba$, we get $ef = 0$ whenever $(ab)^m = 0$, which holds for $m \gg 0$ since $ab \in I$ is nilpotent. Finally, $\bar{f} = \bar{a}^m = \bar{a}$ since $\bar{a}\bar{b} = 0$. Also, $f^2 - f = (f-1)f = ef = 0$.

4. **(10 points)** Let A be an infinite-dimensional simple algebra over a field F. Show that every nonzero left A-module is infinite-dimensional over F.

✎ *Solution*. For any left A-module M, its annihilator $\mathrm{ann}(M)$ is a two-sided ideal. The map $a \mapsto [M \ni m \mapsto am]$ induces an embedding $A/\mathrm{ann}(M) \hookrightarrow \mathrm{End}_F(M)$ of F-algebras. When $M \neq \{0\}$ we must have $\mathrm{ann}(M) = \{0\}$. Were M finite-dimensional, $A = A/\mathrm{ann}(M)$ would be finite-dimensional as well. Contradiction.

5. **(10 points)** Let (V, π) be an absolutely irreducible representation of a finite group G over a field F (notation: V is an F-vector space and $\pi : G \to \mathrm{Aut}_F(V)$). Denote by $Z(G)$ the center of G. Show that there is a group homomorphism $\omega_\pi : Z(G) \to F^\times$, called the *central character* of π, such that $\pi(z) = \omega_\pi(z) \cdot \mathrm{id}_V$ for all $z \in Z(G)$.

✎ *Solution*. Observe that $\pi(z) : V \to V$ belongs to $\mathrm{End}_G(V)$, the latter F-algebra equals F as V is absolutely irreducible. Hence there exists a map $z \mapsto \omega_\pi(z) \in F^\times$ with $\pi(z) = \omega_\pi(z) \cdot \mathrm{id}_V$. From $\pi(z_1)\pi(z_2) = \pi(z_1 z_2)$ one infers that $\omega_\pi : Z(G) \to F^\times$ is a group homomorphism.

6. **(15 points)** Let $H \subset G$ be finite groups, $g \in G$ and (σ, V) be a representation of H over some field F. Set $H^g := g^{-1}Hg$ and consider the g-twisted representation

$$\sigma^g(\cdot) := \sigma(g \cdot g^{-1}) : H^g \to \mathrm{Aut}_F(V)$$

on the same space V. Show that there is an isomorphism of induced representations

$$\mathrm{Ind}_H^G(\sigma) \xrightarrow{\sim} \mathrm{Ind}_{H^g}^G(\sigma^g)$$

given by sending $f : G \to V$ to $f(g\,\cdot) : G \to V$.

✎ *Solution.* It is straightforward to check that $f(g\,\cdot)$ lies in $\mathrm{Ind}_{H^g}^G(\sigma^g)$, and that $f \mapsto f(g\,\cdot)$ defines a homomorphism between induced representations. Its inverse is simply $f' \mapsto f'(g^{-1}\,\cdot)$.

7. **(15 points)** Fix a prime number p. For every q of the form $q = p^n$, $n \in \mathbb{Z}_{\geq 1}$, denote by $\mathbb{F}_q$ the finite field with q elements; thus $\mathbb{F}_q \supset \mathbb{F}_p$. Set

$$\pi_q := \left|\{\alpha \in \mathbb{F}_q : \mathbb{F}_q = \mathbb{F}_p(\alpha)\}\right|.$$

(i) Show that $p^n = \sum_{d|n} \pi_{p^d}$ for all $n \in \mathbb{Z}_{\geq 1}$.

(ii) Infer that $\pi_{p^n} = \sum_{d|n} \mu(d) p^{\frac{n}{d}}$; here μ stands for the Möbius function:

$$\mu(d) = \begin{cases} (-1)^{|\{\text{prime factors of } d\}|}, & d \text{ squarefree}, \\ 0, & \text{otherwise}. \end{cases}$$

✎ *Solution.* As shown in the lecture notes, for every $d|n$ there is exactly one intermediate field $\mathbb{F}_p \subset K \subset \mathbb{F}_{p^n}$ with $[K : \mathbb{F}_p] = d$ (thus $K \simeq \mathbb{F}_{p^d}$), and all intermediate fields are so obtained. The first statement follows by the decomposition into disjoint union

$$\begin{aligned} \mathbb{F}_{p^n} &= \bigsqcup_{d|n} \left\{\alpha \in \mathbb{F}_{p^n} : \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}\right\} \\ &= \bigsqcup_{d|n} \left\{\alpha \in \mathbb{F}_{p^d} : \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}\right\}. \end{aligned}$$

The second statement follows immediately by Möbius inversion formula.