February 28, 2008

Algebra III Final AY2007/8

1. Let $a = \sqrt[5]{2}$, $\zeta = e^{2\pi\sqrt{-1}/5} \in \boldsymbol{C}$, $E = \boldsymbol{Q}(a, \zeta)$, $F = \boldsymbol{Q}(\zeta)$ and $K = \boldsymbol{Q}(a)$. Show the following. (5pts $\times$ 14 = 70pts)

   (a) $\mathrm{Irr}_{\boldsymbol{Q}}(a) = t^5 - 2$.

   (b) $\mathrm{Irr}_{\boldsymbol{Q}}(\zeta) = t^4 + t^3 + t^2 + t + 1$.

   (c) $(E : \boldsymbol{Q}) = \dim_{\boldsymbol{Q}} E = 20$.

   (d) $\mathrm{Irr}_F(a) = t^5 - 2$.

   (e) F is a splitting field of $t^4 + t^3 + t^2 + t + 1$ over $\boldsymbol{Q}$.

   (f) K is not a normal extension of $\boldsymbol{Q}$.

   (g) Every element of E is algebraic over $\boldsymbol{Q}$ and E is a normal extension of $\boldsymbol{Q}$.

   (h) Suppose $\pi : E \to \boldsymbol{C}$ is a ring homomorphism such that $\pi(1) = 1$. Then π is injective and $\pi(m/n) = m/n$ for all integers m, n with $n \neq 0$.

   (i) Suppose $\pi : E \to \boldsymbol{C}$ is a ring homomorphism such that $\pi(1) = 1$. Then $\pi(E) = E$. (Hint: First show that $\pi(a)$ is a root of $t^5 - 2$ and $\pi(\zeta)$ is a root of $t^4 + t^3 + t^2 + t + 1$.)

   (j) There is $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a) = a\zeta$.

   (k) There is $\tau \in \mathrm{Gal}(E/K)$ such that $\tau(\zeta) = \zeta^2$.

   (l) $\mathrm{Gal}(E/\boldsymbol{Q})$ is a non-abelian group.

   (m) Let $\pi \in \mathrm{Gal}(E/\boldsymbol{Q})$. Then $\pi(F) = F$ and the mapping

   $$\phi : \mathrm{Gal}(E/\boldsymbol{Q}) \to \mathrm{Gal}(F/\boldsymbol{Q}) \ (\pi \mapsto \pi_{|F})$$

   is a surjective group homomorphism, where $\pi_{|F}$ denotes the restriction of π to F.

   (n) $\mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/\boldsymbol{Q})$ and $\mathrm{Gal}(E/\boldsymbol{Q})/\mathrm{Gal}(E/F) \simeq \boldsymbol{Z}_4$, a cyclic group of order 4.

2. Let L be a field with 27 elements. Show the following. (5pts $\times$ 6 = 30 pts)

   (a) Every element $x \in L$ satisfies $x^{27} = x$.

   (b) L contains a subfield S with three elements and $x+x+x = 0$ for all elements of $x \in L$. (Hint: Let 1 be the identity element of L. Consider a mapping $\pi : \boldsymbol{Z} \to L\,(n \mapsto n \cdot 1)$.)

   (c) L contains all roots of $t^3 - t + 1 = 0$ and L is normal over S.

   (d) Let $a \in L$ be a root of $t^3 - t + 1 = 0$. Find the order of a, i.e., $\min\{n \in \boldsymbol{N} \mid a^n = 1\}$.

   (e) Let $\sigma : L \to L\ (x \mapsto x^3)$. Then σ is an automorphism of L.

   (f) $\mathrm{Gal}(L/S) = \{id_L, \sigma, \sigma^2\}$.

Hiroshi Suzuki, International Christian University

Solutions to Algebra III Final AY2007/8

1. Let $a = \sqrt[5]{2}$, $\zeta = e^{2\pi\sqrt{-1}/5} \in \boldsymbol{C}$, $E = \boldsymbol{Q}(a, \zeta)$, $F = \boldsymbol{Q}(\zeta)$ and $K = \boldsymbol{Q}(a)$. Show the following. (5pts $\times$ 14 = 70pts)

   (a) $\mathrm{Irr}_{\boldsymbol{Q}}(a) = t^5 - 2$.

   Solution. Since $t^5 - 2$ is irreducible over $\boldsymbol{Q}$ by Eisenstein's criterion and Gauss' lemma, and a is a root of it, we have $\mathrm{Irr}_{\boldsymbol{Q}}(a) = t^5 - 2$.

   (b) $\mathrm{Irr}_{\boldsymbol{Q}}(\zeta) = t^4 + t^3 + t^2 + t + 1$.

   Solution. Since $\zeta^5 = 1$ and $\zeta \neq 1$, ζ is a root of $p(t) = t^4 + t^3 + t^2 + t + 1$. Since $p(t+1) = t^4 + 5t^3 + 10t^2 + 10t + 5$, this is irreducible over $\boldsymbol{Q}$ by Eisenstein's criterion and Gauss' lemma. Hence $p(t)$ itself is irreducible. Therefore $\mathrm{Irr}_{\boldsymbol{Q}}(\zeta) = t^4 + t^3 + t^2 + t + 1$.

   (c) $(E : \boldsymbol{Q}) = \dim_{\boldsymbol{Q}} E = 20$.

   Solution. By (a), $(K : \boldsymbol{Q}) = (\boldsymbol{Q}(a) : \boldsymbol{Q}) = \deg(\mathrm{Irr}_{\boldsymbol{Q}}(a)) = 5$, and by (b) $(F : \boldsymbol{Q}) = (\boldsymbol{Q}(\zeta) : \boldsymbol{Q}) = \deg(\mathrm{Irr}_{\boldsymbol{Q}}(\zeta)) = 4$. Clearly $(E : \boldsymbol{Q}) = (F(a) : F)(F : \boldsymbol{Q}) \leq 20$ as $(F(a) : F) = \deg(\mathrm{Irr}_F(a)) \leq \deg(\mathrm{Irr}_{\boldsymbol{Q}}(a))$ and $(E : \boldsymbol{Q})$ is divisible by 4 and 5. Hence it is 20.

   (d) $\mathrm{Irr}_F(a) = t^5 - 2$.

   Solution. Since a is a root of $t^5 - 2 \in F[t]$, $\mathrm{Irr}_F(a)$ divides $t^5 - 2$. Since $(E : \boldsymbol{Q}) = \dim_{\boldsymbol{Q}} E = 20$, $20 = (E : \boldsymbol{Q}) = (F(a) : F)(F : \boldsymbol{Q}) = \deg(\mathrm{Irr}_F(a)) \cdot 4$, $\deg(\mathrm{Irr}_F(a)) = 5$. Therefore $\mathrm{Irr}_F(a) = t^5 - 2$.

   (e) F is a splitting field of $t^4 + t^3 + t^2 + t + 1$ over $\boldsymbol{Q}$.

   Solution. Since the roots of $p(t) = t^4 + t^3 + t^2 + t + 1$ are $\zeta, \zeta^2, \zeta^3, \zeta^4$, all of them are in F and F is a splitting field of $p(t)$.

   (f) K is not a normal extension of $\boldsymbol{Q}$.

   Solution. $t^5 - 2$ is irreducible over $\boldsymbol{Q}$ by (a), and the roots of it are $a, a\zeta, a\zeta^2, a\zeta^3, a\zeta^4$. Since ζ is not a real number, $K \subset \boldsymbol{R}$ cannot contain all roots. Hence K is not a normal extension of $\boldsymbol{Q}$.

   (g) Every element of E is algebraic over $\boldsymbol{Q}$ and E is a normal extension of $\boldsymbol{Q}$.

   Solution. Let $x \in E$. Since $(E : \boldsymbol{Q}) = 20$, $1, x, x^2, \ldots, x^{20}$ are not linearly independent. Therefore there is a nontrivial linear combination of these elements expressing 0. Hence there is a nonzero polynomial which has x as a root. Thus every element of E is algebraic. As in (f), the roots of $t^5 - 2$ are a, $a\zeta$, $a\zeta^2$, $a\zeta^3$, and $a\zeta^4$. Hence the splitting field of $t^5 - 2$ is $\boldsymbol{Q}(a\zeta, a\zeta^2, a\zeta^3, a\zeta^4) = \boldsymbol{Q}(a, \zeta) = E$. Hence E is normal over $\boldsymbol{Q}$.

(h) Suppose $\pi : E \to \boldsymbol{C}$ is a ring homomorphism such that $\pi(1) = 1$. Then π is injective and $\pi(m/n) = m/n$ for all integers m, n with $n \neq 0$.

Solution. Since π is a ring homomorphism and $\pi(1) = 1$, $\pi(n) = \pi(1) + \cdots + \pi(1) = n$ when n is nongegative. $0 = \pi(0) = \pi(n + (-n)) = \pi(n) + \pi(-n) = n + \pi(-n)$. Hence $\pi(-n) = -n$. Morevover $1 = \pi(n \cdot \frac{1}{n}) = n\pi(\frac{1}{n})$ and $\frac{1}{n} = \pi(\frac{1}{n})$. Thus $\pi(m/n) = m/n$.

(i) Suppose $\pi : E \to \boldsymbol{C}$ is a ring homomorphism such that $\pi(1) = 1$. Then $\pi(E) = E$. (Hint: First show that $\pi(a)$ is a root of $t^5 - 2$ and $\pi(\zeta)$ is a root of $t^4 + t^3 + t^2 + t + 1$.)

Solution. Since $a^5 - 2 = 0$, $0 = \pi(a^5 - 2) = \pi(a)^5 - \pi(2) = \pi(a)^5 - 2$ by (h). Thus $\pi(a)$ is a root of $t^5 - 2$ and $\pi(a) \in \{a, a\zeta, a\zeta^2, a\zeta^3, a\zeta^4\} \subset E$. Similarly $\pi(\zeta)$ is a root of $t^4 + t^3 + t^2 + t + 1$, $\pi(\zeta) \in \{\zeta, \zeta^2, \zeta^3, \zeta^4\} \subset E$. Since $E = \boldsymbol{Q}(a, \zeta)$, $\pi(E) \subset E$. Since π is a $\boldsymbol{Q}$-isomorphism, $(E : \boldsymbol{Q}) = (\pi(E) : \boldsymbol{Q})$ and $\pi(E) = E$.

(j) There is $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a) = a\zeta$.

Solution. By (d), $t^5 - 2$ is irreducible over F and both a and $a\zeta$ are roots of it. Hence there is an isomorphism between $E = F(a)$ and $E = F(a\zeta)$ sending a to $a\zeta$.

(k) There is $\tau \in \mathrm{Gal}(E/K)$ such that $\tau(\zeta) = \zeta^2$.

Solution. Since $(E : K) = 4$ and $E = K(\zeta)$, $\mathrm{Irr}_K(\zeta) = t^4 + t^3 + t^2 + t + 1$. Since both ζ and ζ^2 are roots of an irreducible polynomial $t^4 + t^3 + t^2 + t + 1$, there is an isomorphism from $E = K(\zeta)$ to $E = K(\zeta^2)$ sending ζ to ζ^2. Note that $(\zeta^2)^3 = \zeta \in K(\zeta^2)$.

(l) $\mathrm{Gal}(E/\boldsymbol{Q})$ is a non-abelian group.

Solution. $\tau \circ \sigma(a) = \tau(\sigma(a)) = \tau(a\zeta) = \tau(a)\tau(\zeta) = a\zeta^2$, while $\sigma \circ \tau(a) = \sigma(a) = a\zeta$. Hence $\tau \circ \sigma \neq \sigma \circ \tau$.

(m) Let $\pi \in \mathrm{Gal}(E/\boldsymbol{Q})$. Then $\pi(F) = F$ and the mapping

$$\phi : \mathrm{Gal}(E/\boldsymbol{Q}) \to \mathrm{Gal}(F/\boldsymbol{Q}) \ (\pi \mapsto \pi_{|F})$$

is a surjective group homomorphism, where $\pi_{|F}$ denotes the restriction of π to F.

Solution. First $(F : \boldsymbol{Q}) = 4$ by (b) and (c) and $\pi(\tau) = \tau_{|F} \in \mathrm{Gal}(F/\boldsymbol{Q})$. Note that $\tau(\zeta) = \zeta^2$ and $\tau(F) = F$ as $F = \boldsymbol{Q}(\zeta)$. Since $\tau^2(\zeta) = \tau(\zeta^2) = \tau(\zeta)^2 = \zeta^4$, $\tau^3(\zeta) = \tau(\zeta^4) = \tau(\zeta)^4 = \zeta^8 = \zeta^3$, $\tau^4 = \tau(\zeta^3) = \tau(\zeta)^3 = \zeta$, the order of τ is four. Therefore $\mathrm{Gal}(F/\boldsymbol{Q}) = \langle \phi(\tau) \rangle$. Hence the mapping ϕ is surjective. It is clear that it is a homomorphism as well.

(n) $\mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/\boldsymbol{Q})$ and $\mathrm{Gal}(E/\boldsymbol{Q})/\mathrm{Gal}(E/F) \simeq \boldsymbol{Z}_4$, a cyclic group of order 4.

Solution. Consider the mapping ϕ above. Then $\ker(\phi) = \mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/\boldsymbol{Q})$. Hence we have the assertion by our observation in the previous problem, as π is surjective and $\mathrm{Gal}(F/\boldsymbol{Q}) \simeq \boldsymbol{Z}_4$.

2. Let L be a field with 27 elements. Show the following. (5pts $\times$ 6 = 30 pts)

(a) Every element $x \in L$ satisfies $x^{27} = x$.

Solution. Suppose $x = 0$, then $x^{27} = x$. Hence assume that $x \neq 0$. Since x belongs to the multiplicative group of L of order 26, $x^{26} = 1$. Hence $x^{27} = x$ for all $x \in E$.

(b) L contains a subfield S with three elements and $x+x+x = 0$ for all elements of $x \in L$. (Hint: Let 1 be the identity element of L. Consider a mapping $\pi : \boldsymbol{Z} \to L\,(n \mapsto n \cdot 1)$.)

Solution. Let π be a homomorphism mentioned in Hint. Then it is a ring homomorphism. Since L contains finitely many elements, $\ker \pi \neq 0$, and $\boldsymbol{Z}/\ker \pi$ is isomorphic to a subring of L which does not have any nonzero zerodivisor. Hence $\ker \pi = p\boldsymbol{Z}$ for some prime number p. Thus $\mathrm{Im}\pi$ is a subfield S of L. Since L is a finite extension of S, $|L| = |S|^d = p^d$ for some d. Therefore, $p = 3$ and $x + x + x = 3x = \pi(3)x = 0$.

(c) L contains all roots of $t^3 - t + 1 = 0$ and L is normal over S.

Solution. Let x be a root of $t^3 - t + 1$. Then $x^3 = x - 1$, $x^9 = x^3 - 1 = x + 1$, $x^{27} = x^3 + 1 = x$. Hence x is a root of $t^{27} - t$. Since $t^3 - t + 1$ is irreducible, $t^3 - t + 1$ divides $t^{27} - t$. Since all elements of E are roots of this polynomial of degree 27, $x \in E$.

(d) Let $a \in L$ be a root of $t^3 - t + 1 = 0$. Find the order of a, i.e., $\min\{n \in \boldsymbol{N} \mid a^n = 1\}$.

Solution. The order of a is a divisor of 26 as in (c). Suppose it is not 26. Then it is either 2 or 13. Clearly it is not 2. Since $a^9 = a + 1$ and $a^3 = a - 1$, $a^{13} = (a^2 - 1)a = a^3 - a = -1 \neq 1$. Therefore, the order is 26.

(e) Let $\sigma : L \to L\ (x \mapsto x^3)$. Then σ is an automorphism of L.

Solution. Since $x + x + x = 0$ for all $x \in L$, $(x + y)^3 = x^3 + y^3$ and $(xy)^3 = x^3y^3$. Thus it is a homomorphism. Since $x^3 = 0$ implies $x = 0$, σ is injective. Since $|L|$ is finite, it is injective as well. Therefore, σ is an automorphism of L.

(f) $\mathrm{Gal}(L/S) = \{id_L, \sigma, \sigma^2\}$.

Solution. As we have seen in (a), $x^{27} = x$ for all $x \in L$, $\sigma^3(x) = x^{27} = x$ and the order of σ is three. Since $(L : S) = 3$, we have $\mathrm{Gal}(L/S) = \{id_L, \sigma, \sigma^2\}$.

Hiroshi Suzuki, International Christian University