March 2, 2009

Algebra III Final AY2008/9

1. Let L be a field and let K and F be subfields of L such that $F \subseteq K \subseteq L$.

   (a) Write the definition of that L is algebraic over F. (5pts)

   (b) Write the definition of that L is normal over F. (5pts)

   (c) Show that if L is finite over F, then L is algebraic over F. (10pts)

   (d) If L is algebraic over K and K is algebraic over F, then L is algebraic over F. (10pts)

2. Let p and q be distinct prime numbers, and let $L = \boldsymbol{Q}(\sqrt{p}, \sqrt{q})$ and $G = \mathrm{Gal}(L/\boldsymbol{Q})$.

   (a) Show that L is a normal extension of $\boldsymbol{Q}$. (5pts)

   (b) Show that for $\sigma \in G$, $\sigma(\sqrt{p}) \in \{\sqrt{p}, -\sqrt{p}\}$. (5pts)

   (c) Show that $(L : \boldsymbol{Q}) = 4$. (10pts)

   (d) Find all elements of G. (10pts)

   (e) Show that there are exactly five intermediate fields K satisfying $\boldsymbol{Q} \subseteq K \subseteq L$. (10pts)

3. Let L be a field with 16 elements. Show the following.

   (a) Every element $x \in L$ satisfies $x^{16} = x$. (5pts)

   (b) L contains a subfield K with two elements and $x + x = 0$ for all elements of $x \in L$. (5pts)

   (c) L contains all roots of $t^4 + t + 1 = 0$. (5pts)

   (d) Let $\sigma : L \to L$ $(x \mapsto x^2)$. Then σ is an automorphism of L. (5pts)

   (e) $\mathrm{Gal}(L/K) = \{id_L, \sigma, \sigma^2, \sigma^3\}$. (5pts)

   (f) Let a be a root of $t^4 + t + 1$. Then $Fix(\langle \sigma^2 \rangle) = K(a^5)$. (5pts)

Hiroshi Suzuki, International Christian University

March 2, 2009

Solutions to Algebra III Final AY2008/9

1. Let L be a field and let K and F be subfields of L such that $F \subseteq K \subseteq L$.

   (a) Write the definition of that L is algebraic over F. (5pts)

   Solution. For each element $x \in L$, there is a nonzero polynomial $f(t) \in F[t]$ such that $f(x) = 0$. ■

   (b) Write the definition of that L is normal over F. (5pts)

   Solution. L is algebraic over F and if an irreducible polynomial $f(t) \in F[t]$ has a root in L, then $f(t)$ splits in L, i.e., there exist $c \in F$ and $x_1, x_2, \ldots, x_n \in L$ such that $f(t) = c(t - x_1)(t - x_2)\cdots(t - x_n)$. ■

   (c) Show that if L is finite over F, then L is algebraic over F. (10pts)

   Solution. Since L is finite over F, there exists a positive integer n such that $\dim_F(L) = (L : F) = n$. For $x \in L$, $1, x, x^2, \ldots, x^n$ are not linearly independent. Hence there exist $c_0, c_1, \ldots, c_n$ not all zero such that $c_0 + c_1x + \cdots + c_nx^n = 0$. Let $f(t) = c_0 + c_1t + \cdots + c_nt^n \in F[t]$. By our choice, $f(t) \neq 0$ and $f(x) = 0$. Hence any element $x \in L$ is algebraic over F and L is algebraic over F. ■

   (d) If L is algebraic over K and K is algebraic over F, then L is algebraic over F. (10pts)

   Solution. Let $x \in L$. Then by assumption, there exist $c_0, c_1, \ldots, c_n \in K$ not all zero such that $c_0 + c_1x + \cdots + c_nx^n = 0$, and $f(x) = 0$ by setting $f(t) = c_0 + c_1t + \cdots + c_nt^n \in F[t]$. In particular,

   $$(F(c_0, c_1, \ldots, c_n)(x) : F(c_0, c_1, \ldots, c_n)) \leq \deg(f(t)) \leq n.$$

   Moreover, since $c_0, c_1, \ldots, c_n$ are algebraic over F, $(F(c_0, c_1, \ldots, c_n) : F)$ is finite. Hence $(F(c_0, c_1, \ldots, c_n)(x) : F)$ is finite and x is algebraic over F. Thus any element of L is algebraic over F and L is algebraic over F. ■

2. Let p and q be distinct prime numbers, and let $L = \boldsymbol{Q}(\sqrt{p}, \sqrt{q})$ and $G = \mathrm{Gal}(L/\boldsymbol{Q})$.

(a) Show that L is a normal extension of $\boldsymbol{Q}$. (5pts)

Solution. Clearly L is a splitting field of $f(t) = (t^2 - p)(t^2 - q)$. Hence L is a normal extension of $\boldsymbol{Q}$. ■

(b) Show that for $\sigma \in G$, $\sigma(\sqrt{p}) \in \{\sqrt{p}, -\sqrt{p}\}$. (5pts)

Solution. Since $\sigma(a) = a$ for all $a \in \boldsymbol{Q}$,

$$\sigma(\sqrt{p})^2 = \sigma(\sqrt{p}^2) = \sigma(p) = p.$$

Hence $\sigma(\sqrt{p})$ is a root of a polynomial $t^2 - p$ and hence $\sigma(\sqrt{p}) \in \{\sqrt{p}, -\sqrt{p}\}$. ■

(c) Show that $(L : \boldsymbol{Q}) = 4$. (10pts)

Solution. Since $t^2 - p$, $t^2 - q$ and $t^2 - pq$ are irreducible polynomials over $\boldsymbol{Q}$, $\deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{p})) = \deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{q})) = \deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{pq})) = 2$. Thus

$$(L : \boldsymbol{Q}) = (\boldsymbol{Q}(\sqrt{p})(\sqrt{q}) : \boldsymbol{Q}(\sqrt{p}))(\boldsymbol{Q}(\sqrt{p}) : \boldsymbol{Q}) = \deg(\mathrm{Irr}_{\boldsymbol{Q}(\sqrt{p})}(\sqrt{q}))\deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{p})) \leq 4.$$

Suppose $\deg(\mathrm{Irr}_{\boldsymbol{Q}(\sqrt{p})}(\sqrt{q})) = (\boldsymbol{Q}(\sqrt{p})(\sqrt{q}) : \boldsymbol{Q}(\sqrt{p})) = 1$. Then $\sqrt{q} \in \boldsymbol{Q}(\sqrt{p})$. Since $(\boldsymbol{Q}(\sqrt{p}) : \boldsymbol{Q}) = 2$ and $\deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{q})) = 2$, there exists $a, b \in \boldsymbol{Q}$ with $b \neq 0$ such that $a + b\sqrt{p} = \sqrt{q}$. So $q = a^2 + b^2 p + 2ab\sqrt{p}$ and $ab = 0$. This implies $a = 0$ and $b\sqrt{p} = \sqrt{q}$. Hence $q = b\sqrt{pq}$, which is absurd as $\deg(\mathrm{Irr}_{\boldsymbol{Q}}(\sqrt{pq})) = 2$. Therefore $(L : \boldsymbol{Q}) = 4$. ■

(d) Find all elements of G. (10pts)

Solution. Since $(L : \boldsymbol{Q}) = 4$, $\deg(\mathrm{Irr}_{\boldsymbol{Q}(\sqrt{q})}(\sqrt{p})) = 2$ and $t^2 - p$ is irreducible over $\boldsymbol{Q}(\sqrt{q})$ and $t^2 - q$ is irreducible over $\boldsymbol{Q}(\sqrt{p})$. Therefore there are elements $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{p}))$ such that $\sigma(\sqrt{q}) = -\sqrt{q}$ and $\tau \in \mathrm{Gal}(L/\boldsymbol{Q}(\sqrt{q}))$ such that $\sigma(\sqrt{p}) = -\sqrt{p}$. By our choice, $\sigma(\sqrt{p}) = \sqrt{p}$ and $\tau(\sqrt{q}) = \sqrt{q}$. Since $\tau\sigma(\sqrt{p}) = -\sqrt{p}$ and $\tau\sigma(\sqrt{q}) = -\sqrt{q}$, $id_L, \sigma, \tau, \tau\sigma$ are all distinct. Since $|\mathrm{Gal}(L/\boldsymbol{Q})| \leq (L : \boldsymbol{Q}) = 4$, we have

$$G = \mathrm{Gal}(L/\boldsymbol{Q}) = \{id_L, \sigma, \tau, \tau\sigma\}.$$

Moreover, clearly $\sigma^2 = \tau^2 = (\tau\sigma)^2 = id_L$.

(e) Show that there are exactly five intermediate fields K satisfying $\boldsymbol{Q} \subseteq K \subseteq L$. (10pts)

Solution. Since the characteristic is zero and L is normal over $\boldsymbol{Q}$, L is a Galois extension of $\boldsymbol{Q}$. Therefore there is a one-to-one correspondence between the set of intermediate fields between $\boldsymbol{Q}$ and L and subgroups of G. Since $|G| = 4$, every nontrivial subgroup of G is of order 2 and there are three such subgroups. Including the trivial subgroup and G, there are five in all. ■

3. Let L be a field with 16 elements. Show the following.

(a) Every element $x \in L$ satisfies $x^{16} = x$. (5pts)

Solution. Let x be a nonzero element of L. Then $x^{15} = 1$ as L^* is a multiplicative group of order 15. Hence x is a root of a polynomial $f(t) = t^{16} - t$. Since 0 also satisfies $f(0) = 0$, every element $x \in L$ satisfies $x^{16} - x = 0$ or $x^{16} = x$. ■

(b) L contains a subfield K with two elements and $x + x = 0$ for all elements of $x \in L$. (5pts)

Solution. Let K be the prime field of L. Since L is a finite field, $|K| = p$ for some prime number. Let $(L : K) = n$. Then $16 = |L| = p^n$. Hence $p = 2$ and $n = 4$. The order of K as an additive group is two, $1+1 = 0$ and hence $x+x = (1+1)x = 0x = 0$ for all $x \in L$. ■

(c) L contains all roots of $t^4 + t + 1 = 0$. (5pts)

Solution. Since $|L| = 16$ and all elements of L are roots of $f(t) = t^{16} - t$, L is exactly the set of roots of $f(t)$. Since

$$\begin{aligned} t^{16} - t &= (t^4 + t + 1)(t^{12} + t^9 + t^8 + t^6 + t^4 + t^3 + t^2 + t) \\ &= t(t+1)(t^2 + t + 1)(t^4 + t + 1)(t^4 + t^3 + 1)(t^4 + t^3 + t^2 + t + 1) \end{aligned}$$

L contains all roots of $t^4 + t + 1 = 0$. ■

Note. Let x be a root of $q(t) = t^4 + t + 1$ in a splitting field containing L. Then $(K(x) : K) = 4$ as $q(t)$ is irreducible over K. Thus $|K(x)| = 2^4$ and $x^{16} - x = 0$. Thus $x \in L$. ■

(d) Let $\sigma : L \to L$ $(x \mapsto x^2)$. Then σ is an automorphism of L. (5pts)

Solution. $\sigma(x + y) = (x + y)^2 = x^2 + y^2$ by (b), and $\sigma(xy) = (xy)^2 = x^2y^2 = \sigma(x)\sigma(y)$. Since σ is a nonzero homomorphism from a field, it is injective. Since L is a finite field, it is bijective. Hence σ is an automorphism of L. ■

(e) $\mathrm{Gal}(L/K) = \{id_L, \sigma, \sigma^2, \sigma^3\}$. (5pts)

Solution. By (d), clearly $\sigma \in \mathrm{Gal}(L/K)$. Since every element $x \in L$ satisfies $x^{16} = x$, $\sigma^4(x) = x$. Thus $\sigma^4 = id_L$ and the order of σ divides 4. Moverover $\sigma^2 \neq id$ as otherwise every element of L satisfies $x^4 = \sigma^2(x) = id_L(x) = x$. But $t^4 - t$ has at most 4 roots. Hence this is not the case as $|L| = 16$. ■

(f) Let a be a root of $t^4 + t + 1$. Then $Fix(\langle\sigma^2\rangle) = K(a^5)$. (5pts)

Solution. Since $a^{15} = 1$, the order of a^5 divides 3. But clearly $a \neq 1$. Hence the order of a^5 is three and it is a root of $t^3 - 1 = (t-1)(t^2+t+1)$. Thus $(K(a^5) : K) = 2$. On the other hand, since $|\langle\sigma^2\rangle| = 2$, $(L : Fix(\langle\sigma^2\rangle)) = 2$ and $(Fix(\langle\sigma^2\rangle) : K) = 2$. Since a cyclic group of order 4 has exactly one subgroup of order 2, we have $Fix(\langle\sigma^2\rangle) = K(a^5)$. ■