MATH 259: Homework #5

Jesse Farmer

04 May 2005

1. *Let F be a field with* $\operatorname{char} F \neq 2$.

   (a) *If $K = F(\sqrt{d_1}, \sqrt{d_2})$ where $d_1, d_2 \in F$ have the property that none of d_1, d_2, or $d_1 d_2$ is a square in F, prove that K/F is a Galois extension with* $\operatorname{Gal}(K/F)$ *isomorphic to the Klein 4-group.*

   K is the splitting field of the polynomial $(x^2 - d_1)(x^2 - d_2)$, which is irreducbile as none of d_1, d_2, or $d_1 d_2$ are squares in F, so that K/F is a normal extension. Since $\operatorname{char} F \neq 2$, this polynomial is also separable, so, in fact, K/F is Galois. Consider $\operatorname{Gal}(K/F)$. Any automorphism fixing F is determined completely by its action on the generators $\sqrt{d_1}$ and $\sqrt{d_2}$, which must be mapped to to $\pm\sqrt{d_1}$ and $\pm\sqrt{d_2}$, respectively. S
   ince $[K : F] = 4$, $|\operatorname{Gal}(K/F)| = 4$, so these are, in fact, all the automorphisms. Define $\sigma \in \operatorname{Gal}(K/F)$ by $\sqrt{d_1} \mapsto -\sqrt{d_1}$ and $\sqrt{d_2} \mapsto \sqrt{d_2}$. Similarly, define $\tau \in \operatorname{Gal}(K/F)$ by $\sqrt{d_1} \mapsto \sqrt{d_1}$ and $\sqrt{d_2} \mapsto -\sqrt{d_2}$. Any element of $k \in K$ can be written as

   $$k = a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_1 d_2}$$

   Simple calculation shows that $\sigma(\sqrt{d_1 d_2}) = -\sqrt{d_1 d_2} = \tau(\sqrt{d_1 d_2})$. Furthermore, from their definitions, it is clear that $\sigma^2 = \tau^2 = 1$. Then $\sigma\tau(\sqrt{d_1}) = -\sqrt{d_1}$ and $\sigma\tau(\sqrt{d_2}) = -\sqrt{d_2}$. Hence $\sigma\tau$ is an element of order 2 distinct from σ and τ. But this is a characterization for V_4, the Klein 4-group: a group of order 4 whose nonidentity elements each have order 2. Hence $\operatorname{Gal}(K/F) \cong V_4$.

   (b) *Conversely, suppose that K/F is a Galois extension with* $\operatorname{Gal}(K/F)$ *isomorphic to the Klein 4-group. Prove that $K = F(\sqrt{d_1}, \sqrt{d_2})$ where $d_1, d_2 \in F$ have the property that none of d_1, d_2, or $d_1 d_2$ is a square in F.*

   Note that because K/F is Galois, $[K : F] = 4$. Every subgroup of V_4 is normal, and therefore there exist three distinct intermediary fields E between K and F. Furthermore, since each element in V_4 has order 2, it follows that $[E : F] = 2$ for all such E. That is, every intermediary field is a quadratic extension of F. In particular, there exist d_1, d_2 such that $E_1 = F(\sqrt{d_1})$ and $E_2 = F(\sqrt{d_2})$ where neither d_1 nor d_2 are squares. Hence $K = F(\sqrt{d_1}, \sqrt{d_2})$ since E_1 and E_2 are distinct. $\sqrt{d_1 d_2} \notin F$ since, otherwise, $[K : F]$ would be 3.

2. (a) *Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.*

   This polynomial is irreducible since it is Eisenstein at 2.

   (b) *Show the roots of this quartic are of the form*

   $$\alpha_1 = \sqrt{1 + \sqrt{3}} \quad \alpha_3 = -\sqrt{1 + \sqrt{3}}$$
   $$\alpha_2 = \sqrt{1 - \sqrt{3}} \quad \alpha_4 = -\sqrt{1 - \sqrt{3}}$$

   Obviously α_1 is a root if and only if α_3 is, and similarly for α_2 and α_4. But

   $$\alpha_1^4 = 4 + 2\sqrt{3} \text{ and } \alpha_1^2 = 1 + \sqrt{3}$$

   so $\alpha_1^4 - 2\alpha_1^2 - 2 = 0$. It is exactly the same for α_2.

(c) *Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) := F$.*

Clearly $K_1 \neq K_2$ since the former is a subfield of the reals and the latter is not. Then since $\mathbb{Q}(\sqrt{3}) \subset K_1 \cap K_2$,

$$4 = [K_1 : \mathbb{Q}] = [K_1 : K_1 \cap K_2][K_1 \cap K_2 : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

But $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 1$ and $[[K_1 : K_1 \cap K_2] > 1$ since $K_1 \neq K_2$, so that $[[K_1 \cap K_2 : \mathbb{Q}(\sqrt{3})] = 1]$.

(d) *Prove that K_1, K_2, and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.*

Over F, the minimal polynomials of α_1 and α_2 are $x^2 - \sqrt{3} - 1$ and $x^2 + \sqrt{3} - 1$, respectively, both of which split. Hence K_1 and K_2 are Galois. K_1K_2 is the splitting field of $x^4 - 2x^2 - 2$ over F, and is therefore also Galois.

$\mathrm{Gal}(K_1K_2/F) \cong V_4$, which can be seen by writing out the element of the automorphism group explicitly. First, any automorphism must send α_1 to $\pm\alpha_1$, and similarly, must send α_2 to $\pm\alpha_2$. Moreover, an automorphism is uniquely defined by its action on the generators. Define $\sigma \in \mathrm{Gal}(K/F)$ by $\alpha_1 \mapsto -\alpha_1$ and $\alpha_2 \mapsto \alpha_2$. Similarly define $\tau \in \mathrm{Gal}(K/F)$ by $\alpha_1 \mapsto \alpha_1$ and $\alpha_2 \mapsto -\alpha_2$. Then $\sigma^2 = \tau^2 = 1$, and furthermore, $\sigma\tau$ acts by sending both α_1 and α_2 to their additive inverses. Hence $(\sigma\tau)^2 = 1$ and $\sigma\tau$ is the fourth element. There are no more automorphisms since we know $|\mathrm{Gal}(K/F)| = 4$, and therefore $\mathrm{Gal}(K/F) \cong V_4$.

(e) *Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.*

Let K/F be the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$. From the previous part we know that $K = F(\alpha_1, \alpha_2)$. Furthermore, from the previous parts, it follows that $[K : F] = 8$ since $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Define an automorphism by the cycle $(\alpha_1\,\alpha_2\,\alpha_3\,\alpha_4)$, and a second automorphism by $(\alpha_1\,\alpha_2)(\alpha_3\,\alpha_4)$. But the group generated by these two permutations is precisely the dihedral group D_8, which can be seen by treating the former as a rotation of a square with vertices labeled clockwise from the northwest corner as $\alpha_1, \alpha_2, \alpha_3$, and α_4, and the latter as a reflection about the vertical axis of symmetry.

3. *Let F be a field and $f = x^p - a$, $a \in F$ and p a prime. Show that f is reducible in $F[x]$ if and only if f has a root in F.*

That this condition is necessary is obvious, since if f has a root then it factors into $(x - r)g$ for some $r \in F$ and $g \in F[x]$.

The converse was already shown for $\mathrm{char}\, F = p$, so assume $\mathrm{char}\, F \neq p$. Then $x^p - a$ only has simple roots since the derivative px^{p-1} has only one $(p-1)$-fold root: zero. Let E/F be the splitting field of f over F so that $E = (\alpha, \zeta)$, where ζ is a primitive n^{th} root of unity and $\alpha \in E$ is some root of $x^p - a$. Write

$$f(x) = \prod_{i=0}^{p-1} (x - \zeta^i \alpha)$$

Suppose f is reducible. If $\alpha \in F$ then we are done, so assume $\alpha \in E \setminus F$. Let g be the minimal polynomial of α over F and $\deg g = r$. Then $1 < r < p$ and

$$g(x) = \prod_{k=1}^{r} (x - \zeta^{i_k} \alpha)$$

where $\{i_k\}$ is just some subset of $\{1, \ldots, p-1\}$. From a quick calculation we see that the constant term in g must be $\pm\zeta^l \alpha^r \in F$ for some $l \geq 0$. Then, in either case, $\zeta^l \alpha^r \in F$. Since $(r, p) = 1$ and $\zeta \in \mu_p$, a group of order p, there exists some $\zeta' \in \mu_p$ such that $\zeta = \zeta'^r$. Then $\zeta'^{rl} \alpha^r = (\zeta'^l \alpha)^r \in F$. Also $(\zeta'^l \alpha)^p = \alpha^p = a \in F$. From these two equations it follows that $\zeta'^l \alpha \in F$. But $\zeta' \alpha$ is a root of f, and we are done.

4. *Let E/F be a finite extension. Show that E/F is a simple extension if and only if the number of intermediary subfields between F and E are finite.*

   Suppose E is simple with $E = F(\alpha)$ and $[E : F] = n < \infty$. Let f be the minimal polynomial of α over F. Let T be the set of all intermediary subfields between F and E, and let $T' = \{g \in E[x] \mid g \text{ monic and } g \mid f\}$. Then T' is finite (in fact, of cardinality less than or equal to 2^n). For $K \in T$ let f_K be the minimal polynomial of α over K. Define a function $T \to T'$ by $K \mapsto f_K$. We claim this is injective. Assume $f_K = f_L = g$ for $K, L \in T$. Then the coefficients of g reside in $K \cap L$, so g is also the minimal polynomial of α over $K \cap L$. But since $(K \cap L)(\alpha) = E$, it follows that $[K : K \cap L] = 1$ and $[L : K \cap L] = 1$ and hence $K = L$. Therefore $|T| \leq |T'| \leq 2^n$.

   To prove the converse, assume T from above is finite. We may assume without loss of generality that F is infinite, since a finite extension of a finite field is simple. Let $\alpha \in E$ such that $[F(\alpha) : F]$ is maximal among all simple subextensions of E/F. Assume for contradiction that $F(\alpha) \neq E$, and choose $\beta \in E \setminus F(\alpha)$. Consider all subfields of the form $F(\alpha + c\beta)$ for $c \in F$. Since F is infinite, it follows from the pigeonhole principle that there exist distinct $c, c' \in F$ such that $F(\alpha + c\beta) = F(\alpha + c'\beta)$. Immediately we see that this implies $\beta \in F(\alpha + c\beta)$ (since $(c - c')\beta$ is an element), which in turn implies $\alpha \in F(\alpha + c\beta)$. Hence $F(\alpha, \beta) = F(\alpha + c\beta)$. But $[F(\alpha, \beta) : F] > [F(\alpha) : F]$, contradicting the maximality of the latter. Therefore $E = F(\alpha)$.

5. *Let p be a prime number and $E = F(\alpha)$ where $\alpha^p = a \in F^*$ and $x^p - a$ irreducible. Suppose* $\operatorname{char} F \neq p$, *and let $\beta \in E$. Show that $\beta^p = b \in F$ if and only if $\beta = c\alpha^i$ for some $c \in F$ and $i \geq 0$.*

6. *Compute $[\mathbb{Q}(\sqrt[p]{2}, \sqrt[p]{3}) : \mathbb{Q}]$, where p is a prime.*

7. *Show that $\mathbb{Q}(\sqrt[p]{2}, \sqrt[p]{3}) = \mathbb{Q}(\sqrt[p]{2} + \sqrt[p]{3})$.*

8. *Let $E/\mathbb{Q}$ be the splitting field of $x^p - 3$, where p is a prime. Show that* $\operatorname{Gal}(E/\mathbb{Q})$ *has a normal cyclic subgroup of order p with quotient an abelian group of order $p - 1$.*