MATH 259: Homework #6

Jesse Farmer

11 May 2005

1. *Let E/F be a field extension with $|F| < \infty$ and $[E : F] = n$. Show that there exists a subfield $E' \subset E$ with $[E' : F] = d$ if and only if $d \mid n$, and that this E' is unique. Conclude that there exists a subfield E' of E with $|E'| = p^d$ if and only if $d \mid n$.*

   I assume that $|F| = p$, p a prime number, since otherwise the rest of the exercise does not work. Then $\mathrm{Gal}(E/F)$ is cyclic of order n, and from group theory we know that $d \mid n$ if and only if there exists a subgroup H of $\mathrm{Gal}(E/F)$ of order d, and that any such subgroup is unique. Writing $G = \mathrm{Gal}(E/F)$, the fixed field E' of H is therefore the unique field such that $[E' : F] = |G : H| = \frac{n}{d} = a \in \mathbb{Z}$. Of course, this suffices, as $\frac{n}{d} = a$, so that $d \mid n$ if and only if $a \mid n$.

   Let E be as above, then $|E| = p^n$. From above $[E' : F] = d$ if and only if $d \mid n$, which is true if and only if $|E| = p^d$, since E' is the splitting field of $x^{p^d} - x$.

2. *Let F be a finite field with $|F| = q$ and $[E : F] = n$. Let $R_d(F)$ be the set of all monic irreducible polynomials of degree d in $F[x]$. Show that*

$$x^{q^n} - x = \prod_{d \mid n} \left(\prod_{f \in R_d(F)} f \right)$$

   If $\alpha \in E$ is a root of $x^{q^n} - x$ then its minimal polynomial over F must have degree d dividing n, and hence is in $R_d(F)$ for the appropriate d.

   To show the converse, note that any two monic irreducible factors of the same degree in the right-hand polynomial must have the same splitting field by the uniqueness derived in the first question. Since at least one polynomial of degree $d \mid n$ splits, then, it follows that every polynomial of degree $d \mid n$ splits in E. Moreover, from the construction of $\mathbb{F}_{q^n}$, any polynomial which splits in E must have linear factors that are also factors of $x^{q^n} - x$. Hence the right-hand polynomial divides $x^{q^n} - x$.

3. *Let E/F be a Galois extension with $[E : F] = n$. Suppose p is a prime such that $p \mid n$. Show that there is a subfield F' of E with $F \subset F' \subset E$ and $[F' : F] = \frac{n}{p}$. Furthermore, show that if $n = p^r m$ where $p \nmid m$ then there exists a subfield F' as above with $[E : F'] = p^r$.*

   Consider $G = \mathrm{Gal}(E/F)$. $|G| = n$, so by Cauchy's theorem for every $p \mid n$ there exists an element of order $p \in G$. In particular, the subgroup generated by this element has order p, so there exists $H \leq G$ with $|H| = p$. Let K be the fixed field of H. Then the fundamental theorem says $\frac{n}{p} = |G : H| = [K : F]$, so K is precisely the field for which are are looking.

   Now assume that $n = p^r m$ where $p \nmid m$. Then from Sylow's theorem we know there exists a Sylow p-subgroup H of $G = \mathrm{Gal}(E/F)$ of order p^r. Let K be the fixed field of this subgroup. Then $p^r = |H| = [E : K]$, so, again, K is precisely the field for which are are looking.

4. *Let $E/\mathbb{Q}$ be a finite normal extension. Suppose $\sqrt[3]{p} \in E$ where p is prime. Show that $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian.*

To show the contrapositive assume that $\text{Gal}(E/\mathbb{Q})$ is abelian. Then every subgroup is normal, and each corresponding fixed field is a Galois extension. However, $\mathbb{Q}(\sqrt[3]{p})$ is easily seen to not be Galois since the splitting field of $x^3 - p$, which is monic irreducible since it is Eisenstein at p, contains one real root and two purely complex roots and $\mathbb{Q}(\sqrt[3]{p})$ is a subset of the reals. Hence it is not a normal extension, and the corresponding subgroup of $\text{Gal}(E/\mathbb{Q})$ is not normal. Therefore $\sqrt[3]{p} \notin E$.

5. *Let E/F be a cyclic extension of degree n. Show that for all $d \mid n$, $d > 0$, there exists a cyclic extension F'/F with $F' \subset E$ such that $[F' : F] = d$.*

   Let $G = \text{Gal}(E/F) \cong \mathbb{Z}/n\mathbb{Z}$. By the fourth isomorphism theorem for groups, for $d \mid n$,

   $$d\mathbb{Z}/n\mathbb{Z} \trianglelefteq \mathbb{Z}/n\mathbb{Z}$$

   By the fundamental theorem of Galois theory there exists a cyclic Galois extension F' of F with $[F' : F] = |d\mathbb{Z}/n\mathbb{Z} : \mathbb{Z}/n\mathbb{Z}| = d$.

6. *Let E/F and E'/F be field extensions with $|E| = |E'| < \infty$. Prove or disprove that there is an F-isomorphism $\sigma : E \to E'$.*

   Let f and f' be the polynomials of which E and E' are splitting fields, respectively, which exist because any finite extension of a finite field is normal. Consider the splitting field K of ff'. Then $[K : E], [K : E'] \mid n$ and $[K : E] = [K : E']$. Hence, by the uniqueness part of the first exercise, $E = E'$ and there certainly exists an F-isomorphism between these two fields.

7. *Let $E = \mathbb{Q}(\sqrt[4]{p})$, p a prime. Let $\beta \in E$ be such that $\beta^4 \in \mathbb{Q}$. Show that $\beta = c(\sqrt[4]{p})^i$ for some $c \in \mathbb{Q}$ and $i \geq 0$.*

8. *Compute $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{3})$ and $\mathbb{Q}(\sqrt[4]{2} + \sqrt[4]{3})$.*

   I don't know what this question means. Does it mean compute the Galois group? Or perhaps compute the degree of the extension?

9. *Let p be a prime and $E/\mathbb{Q}$ the splitting field of $x^p - 1$. Show that $E/\mathbb{Q}$ is a cyclic extension of degree $p - 1$.*

   $x^p - 1$ is reducible over $\mathbb{Q}$ into $(1 - x)(1 + \cdots x^{p-1})$. Hence the splitting field of $x^p - 1$ is of degree $p - 1$. Furthermore, $\text{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, which for p prime is cyclic of order $p - 1$.

10. *Let E_n be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Show that $\sqrt[3]{2} \notin E_n$ for all $n \geq 1$.*

    Write $E_n = \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n^{th} root of unity. Then by Theorem 26 in chapter 14 of Dummit and Foote, $\text{Gal}(E_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of units of $Z/n\mathbb{Z}$. In particular, $E_n/\mathbb{Q}$ is a finite normal abelian extension. Since it is abelian $\sqrt[3]{2} \notin E_n$ by fourth exercise.

11. *Let $E_n/\mathbb{Q}$ be as above. Let $\sigma \in \text{Gal}(E_n/\mathbb{Q})$, and write $E = \mathbb{Q}(\zeta)$ where ζ is a primitive n^{th} root of unity. Suppose $\sigma(\zeta) = \zeta^a$. Show that for all $\eta \in \mu_n$, $\sigma(\eta) = \eta^a$. Furthermore, a and n are relatively prime.*

    Since $\mu_n = \langle \zeta \rangle$, write $\eta = \zeta^b$ for some $b < n$. Then

    $$\sigma(\eta) = \sigma(\zeta^b) = \sigma(\zeta)^b = \zeta^{ba} = \left(\zeta^b\right)^a = \eta^a$$

    Assume $\gcd(a, n) = d > 1$. Then $\sigma(1) = 1$ and

    $$\sigma(\zeta^{\frac{n}{d}}) = \zeta^{\frac{na}{d}} = 1$$

    since $\frac{a}{d} = k \in \mathbb{Z}$. Hence σ is not injective, and therefore certainly not a bijection.

12. *Let E be the splitting field of $x^{15}-1$ over $\mathbb{Q}$. Determine $[E:\mathbb{Q}]$ and $\varphi_{15}(x)$, the minimal polynomial of ζ over $\mathbb{Q}$, where $E=\mathbb{Q}(\zeta)$ and $\zeta^{15}=1$.*

    $[E:\mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})| = \varphi(15)$, where φ is Euler's totient function. But $\varphi(15)=8$. Factoring $x^{15}-1$ over $\mathbb{Q}$ gives

$$x^{15}-1 = (x-1)(1+x+x^2)(1+x+x^2+x^3+x^4)(1-x+x^3-x^4+x^5-x^7+x^8)$$

    hence $\varphi_{15} = 1-x+x^3-x^4+x^5-x^7+x^8$.