# MATH 259: Homework #7

Jesse Farmer

18 May 2005

1. *Let $K/F$ be a Galois extension with* $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. *How many intermediate fields $L$ are there such that:*

   (a) $[L : F] = 4$

   By FTG it is sufficient and necessary to find subgroups $H$ of $\mathrm{Gal}(K/F)$ with index 4, i.e., subgroups of order 6. Let $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} = \langle x, y | x^2 = y^{12} = 1, xyx^{-1}y^{-1} = 1\rangle$. The only subgroups of order 6 are therefore $\langle y^6 \rangle$ and $\langle xy^4 \rangle$. Therefore there exist two intermediate fields $L$ such that $[L : F] = 4$.

   (b) $[L : F] = 9$

   As $9 \nmid 24$, there are no such fields.

   (c) $\mathrm{Gal}(K/L) \cong \mathbb{Z}/4\mathbb{Z}$

   Using the same presentation as in (a), it is easy to see that the only possible subgroups of order 4 are $\langle y^3 \rangle, \langle x, y^6 \rangle$, and $\langle xy^3 \rangle$. Only the first and last are cyclic, and therefore are isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Hence there are two such intermediate fields.

2. (a) *Let $F$ be a field with* $\mathrm{char}\, F = p > 0$, $f = x^p - x + a \in F[x]$. *Let $E/F$ be a field extension with $\alpha \in E$ where $f(\alpha) = 0$. Show that $\alpha, \alpha + 1, \ldots, \alpha + (p - 1)$ are all roots of $f$.*

   Let $1 \le n \le p - 1$ and assume $f(\alpha) = 0$. Then

   $$f(\alpha + n) = (\alpha + n)^p - \alpha - n + a = \alpha^p + n^p - \alpha - n + a = n^p - n = 0$$

   Since $p \mid n^p - n$ by Fermat's Little Theorem.

   (b) *With $F$ and $f$ as above, show that $f$ is irreducible over $F$ if and only if $f$ has no roots in $F$.*

   By the first part if $f$ has any root in $F$ then $f$ has all of its roots in $F$, and therefore $f$ is reducbile. Indeed, it splits completely into linear factors over $F$.

   Assume $f$ has no roots in $F$. Let $E/F$ be the splitting field of $f$ and suppose for contradiction that $f = gh$, $g, h \in F[x]$ with $\deg g = r < p$, i.e., $f$ is reducible. Hence $gh = \prod_{i=0}^{p-1}(x - \alpha - i)$ by the first part. Write $g(x) = x + cx^{r-1} + \cdots c_0$. Calculating $c$ gives $c = r\alpha + b$ for some $b \in F$, and hence $\alpha \in F$, a contradiction.

   (c) *With $F$ and $f$ as above, suppose $f$ has no roots in $F$. Let $E/F$ be the splitting field of $f$ over $F$. Show that $E = F(\alpha)$ for all $\alpha \in E$ such that $f(\alpha) = 0$ and $E/F$ is cyclic of degree $p$. Exhibit the elements of* $\mathrm{Gal}(E/F)$.

   Let $\alpha \in E$ such that $f(\alpha) = 0$. Then from the first part $\alpha + 1, \cdots, \alpha + (p - 1)$ are also roots, each of which is clearly in $E$. Since $\deg f = p$ these are all the roots and therefore $E = F(\alpha)$.

   Let $E = F(\alpha)$. Then $p = [E : F] = |\mathrm{Gal}(E/F)|$. Define $\sigma \in \mathrm{Gal}(E/F)$ by $\sigma(\alpha) = \alpha + 1$. Then $|\sigma| = p$ and hence $\mathrm{Gal}(E/F) = \langle \sigma \rangle$, i.e., $\mathrm{Gal}(E/F)$ is cyclic of degree $p$.

3. *Determine the Galois group of $x^4 + x^2 + 4$ over $\mathbb{Q}$.*

4. (a) *Suppose $H \trianglelefteq S_4$ and $S_3 \leq H$. Show that $H = S^4$.*

   Let $H$ be such that $S_3 \leq H \trianglelefteq S_4$. Since $H$ is normal it contains all conjugates of transpositions in $S_3$. But it is easy to see that this requires $H$ to contain all transpositions in $S_4$ since for $(ab) \in S_3$ and $(cd) \in S_4$, distinct transpositions, conjugating $(ab)$ by $(acbd)$ gives $(cd)$. Hence $H = S_4$.

   (b) *Let $E/F$ be a Galois extension with $G = \mathrm{Gal}(E/F) \cong S_4$ via $\eta : S_4 \to G$. Let $H = \eta(S_3)$. Let $F'$ be the fixed field of $H$. Compute $[F' : F]$. Show that for any intermediate field $L$ either $L = F'$ or $L = F$.*

   First, $[F' : F] = |S_4 : S_3| = 4$. Assume $F \subsetneq L \subsetneq F'$, since otherwise we are done. By the Galois correspondence $H$, the elements in $\mathrm{Gal}(E/F)$ fixing $L$ is isomorphic to a proper subgroup of $S_4$ properly containing $S_3$. But if this is so then $|H| = 12$ and $|\mathrm{Gal}(E/F) : H| = 2$. Hence $H$ is normal, and by the first part $H \cong S_4$. It then follows that $L = F$.

5. *Given any monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree at least one show that there are infinitely many distinct prime divisors of the integers $f(1), f(2), \ldots, f(n), \ldots$.*

   Assume for contradiction that there exist a finite number of primes $p_1, \ldots, p_k$ which divide each of $f(1), \ldots, f(n)$. Let $N \in \mathbb{Z}$ such that $f(N) = a \neq 0$ and let $\beta = ap_1p_2 \cdots p_k$. Define

$$g(x) = a^{-1} f(N + \beta x)$$

   Every term in $f(N + \beta x)$ has a coefficient containing $\beta$ except the constant term, which is exactly

$$N^n + a_{n-1}N^{n-1} + \cdots + a_0 = f(N) = a$$

   Hence each term is divisible by $a$ and $g(x) \in \mathbb{Z}[x]$. Furthermore, since each term containing $\beta$ is congruent to $0 \mod p_1 \cdots p_k$, and the constant term of $g$ is just 1, it must be the case that

$$g(n) \equiv 1 \mod p_1p_2 \cdots p_k$$

   for $n \in \mathbb{Z}_+$.

   If $g(b) = 1$ for all $n \in \mathbb{Z}_+$ then $f$ would be the constant polynomial, contradicting the hypothesis that $\deg f \geq 1$. So there exists an $m$ with $g(m) \neq 1$. Since $g(m) \equiv 1 \mod p_1 \cdots p_k$, $g(m) \equiv 1 \mod p_i$ for all $1 \leq i \leq k$. In particular this means that none of the $p_i$ divide $g(m)$. Since $g(m) \neq 1$ it must be divisible by a prime number not among the $p_i$ and therrefore $f(N + \beta m)$ has a prime factor not among the $p_i$, also.

6. *Let $p$ be an odd prime not dividing $m$ and let $\Phi_m(x)$ be the $m^{th}$ cyclotomic polynomial. Suppose $a \in \mathbb{Z}$ satisfies $\Phi_m(a) \equiv 0 \mod p$. Prove that $a$ is relatively prime to $p$ and that the order of $a$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is precisely $m$.*

   Write

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \Phi_m(x) \prod_{\substack{d|m \\ d<m}} \Phi_d(x)$$

   If $\Phi_m(a) = 0$ then $a^m \equiv 1 \mod p$. The only possible divisors of $p$ are 1 and $p$, so if $\gcd(a, p) \neq 1$ then $\gcd(a, p) = p$. But then $a^m \equiv 0 \mod p$ so that $1 \equiv 0 \mod p$, which is absurd.

   Assume for contradiction that the order of $a$ is less than $m$, so that there exists a $d < m$ with $a^d \equiv 1 \mod p$. Then $a$ would be a root of $\Phi_m(x)$ and $\Phi_d(x)$, which would mean that $x^m - 1$ is not separable – a contradiction since $p \nmid m$.

7. *Let $a \in \mathbb{Z}$. Show that $p$ is an odd prime dividing $\Phi_m(a)$ then either $p \mid m$ or $p \equiv 1 \mod m$.*

8. *Prove there are infinitely many primes $p$ with $p \equiv 1 \mod m$.*

   There are infinitely many odd primes, and only finitely many primes dividing $m$. From the previous exercises we know that there are infinitely many primes dividing $\Phi_m(a)$ for $a \in \mathbb{Z}_+$, and since there are only finitely many primes dividing $m$, there are infinitely many primes not dividing $m$ which do divide $\Phi_m(a)$. Hence there are infinitely many such that primes $p$ such that $p \equiv 1 \mod m$.

9. *Deduce that if $G$ is any finite abelian group then there exists a Galois extension $E/\mathbb{Q}$ such that* $\mathrm{Gal}(E/\mathbb{Q}) \cong G$.

By the fundamental theorem of finite abelian groups

$$G \cong \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$

for some integers $n_1, \ldots, n_r$. By the previous exercise there exist $r$ distinct primes such that $p_i \equiv 1 \mod n_i$. Let $L/\mathbb{Q}$ be the splitting field of $x^m - 1$ for $m = p_1 p_2 \cdots p_k$. Then

$$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^\times$$

Thus $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{i=1}^{r} G_i$ where $G_i$ is a cyclic group of order $p_i - 1$. For each $n_i \mid (p_i - 1)$ there exists $H_i \trianglelefteq G_i$ with $|H_i| = \frac{p_i - 1}{n_i}$. Hence $G_i/H_i$ is cyclic of order $n_i$. Recall from group theory that for groups $\{G_i\}$ and normal subgroups $\{H_i \leq G_i\}$ that

$$\frac{\prod_{i=1}^{k} G_i}{\prod_{i=1}^{k} H_i} \cong \prod_{i=1}^{k} G_i/H_i$$

by consideration of the first isomorphism theorem. Let $H = \prod_{i=1}^{r} H_i$ and $E$ the fixed field of $H$. Then by the above

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \frac{\prod_{i=1}^{r} G_i}{\prod_{i=1}^{r} H_i} \cong \prod_{i=1}^{r} G_i/H_i \cong \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \cong G$$