MATH 601: Abstract Algebra II
6th Homework
Partial Solutions

Jonathan Rosenberg

assignment due Wednesday, March 28, 2001

1 Hungerford Problems

V, Section 7, Exercise 6.b. Show that if K is a field of characteristic p and there exists a cyclic extension of degree p of K, then there exists a cyclic extension of degree p^n of K, for all $n \geq 1$.
Solution. We prove this by induction on n, the case of $n = 1$ being trivial. Assume the result is true for $n-1$, so there is a field E cyclic over K of degree p^{n-1}. Choose a generator σ of $\mathrm{Gal}(E/K)$. Since E is separable over K, $T^E_K : E \to K$ is a non-trivial K-linear map, and since $\dim_K K = 1$, T^E_K is therefore surjective. So there is an element $v \in E$ with $T^E_K(v) = 1$. In more concrete terms,

$$v + \sigma(v) + \cdots + \sigma^{p^{n-1}-1}(v) = 1.$$

Clearly $v \notin K$, since otherwise we'd have $T^E_K(v) = [K : E]v = p^{n-1}v = 0$ (since we're in characteristic p), so in particular $v^p \neq v$. Since σ commutes with the endomorphism $x \mapsto x^p$,

$$T^E_K(v^p) = v^p + \sigma(v^p) + \cdots + \sigma^{p^{n-1}-1}(v^p) = \Big(v + \sigma(v) + \cdots + \sigma^{p^{n-1}-1}(v)\Big)^p = 1^p = 1.$$

So $T^E_K(v^p - v) = 1 - 1 = 0$ and by the additive analogue of Hilbert's Theorem 90, there is an element $u \in E$ with $\sigma(u) - u = v^p - v$. We claim $x^p - x - u \in E[x]$ is irreducible. For if not, we know from Hungerford Corollary V.7.9 that $w^p - w - u = 0$ for some $w \in E$. Then $v^p - v = \sigma(u) - u = \sigma(w^p - w) - (w^p - w)$ and so

$$\big(v - \sigma(w) + w\big)^p = v - \sigma(w) + w,$$

i.e., $v - \sigma(w) + w$ lies in the fixed field of $x \mapsto x^p$, which is $\mathbb{F}_p \subseteq K$. So for some $j \in \mathbb{F}_p$, $\sigma(w) = v + w + j$. By iteration, we get $\sigma^2(w) = \sigma(v + w) + j = \sigma(v) + v + w + 2j$, and so

$$\sigma^{p^{n-1}}(w) = \big(v + \sigma(v) + \cdots + \sigma^{p^{n-1}-1}(v)\big) + w + p^{n-1}j = T^E_K(v) + w = w + 1.$$

Since σ had order p^{n-1}, this is a contradiction. So $x^p - x - u \in E[x]$ is irreducible. Let w be a root; then $E(w)$ is cyclic over E of order p, and of degree $[E(w) : E][E : K] = p \cdot^{n-1} = p^n$ over K. We claim $E(w)$ is cyclic over K of order p^n. Indeed, if we define $\widetilde{\sigma}$ to be σ on E and to send $w \mapsto w + v$, then the calculation above shows that $\widetilde{\sigma}$ is an automorphism of $E(w)$ extending σ on E and with the property that $\widetilde{\sigma}^{p^{n-1}}(w) = w + 1$, so that $\widetilde{\sigma}^{p^{n-1}}$ generates $\mathrm{Gal}(E(w)/E)$. So $\widetilde{\sigma}$ has order p^n and generates $\mathrm{Gal}(E(w)/K)$. This proves that $E(w)$ is Galois over K with cyclic Galois group. □

2 Additional Exercises

2. Let K be a finite field with q elements, and let L be a finite extension field with $[L : K] = r$. (Thus L has qr elements.) Recall that the multiplicative groups $L^\times$ and $K^\times$ are cyclic, and that $G = \mathrm{Gal}(L/K)$ is also cyclic. Compute the norm map $N^L_K : L^\times \to K^\times$ explicitly, and show that it is surjective. Show that your calculation agrees with the prediction of Hilbert's Theorem 90.
Solution. Recall that G is cyclic of order r, with generator the *Frobenius automorphism* $\sigma : x \mapsto x^q$. For an element $x \in L^\times$, the norm is given by

$$N^L_K(x) = \prod_{i=0}^{r-1} \sigma^i(x) = \prod_{i=0}^{r-1} x^{q^i} = x^{\sum_{i=0}^{r-1} q^i} = x^{(q^r-1)/(q-1)}.$$

In particular $N^L_K : L^\times \to K^\times$ is a homomorphism. If x_0 is a generator of $L^\times$, then x_0 has order $q^r - 1$ and $\left(N^L_K(x_0)\right)^j = 1$ exactly when $j(q^r - 1)/(q - 1)$ is divisible by $q^r - 1$, i.e., when $(q - 1) \mid j$. That shows $N^L_K(x_0)$ has order exactly $q - 1$ and is thus a generator of $K^\times$, so $N^L_K : L^\times \to K^\times$ is surjective. Then by the isomorphism theorems, $K^\times \cong L^\times/\ker N^L_K$, so $\ker N^L_K$ has order $|L^\times|/|K^\times| = (q^r - 1)/(q - 1)$. Now Hilbert's Theorem 90 claims that the kernel of the normal map should consist of elements of the form $\sigma(y)/y$. Since $\sigma(y)/y = y^q/y = y^{q-1}$ and $(q - 1) \mid |L^\times|$, $\ker N^L_K$ should have order $|L^\times|/(q - 1) = (q^r - 1)/(q - 1)$, which is just what we showed. □

3. Let K be the splitting field over $\mathbb{Q}(\omega)$, ω a primitive cube root of unity, of the polynomial $x^3 - 3x + 1$. Show that K is a cyclic extension of $\mathbb{Q}(\omega)$ of degree 3, and use the Lagrange resolvant method to show it's obtained by adjoining a cube root of something. Again write down the norm map $K^\times \to \mathbb{Q}(\omega)^\times$ explicitly and verify the conclusion of Hilbert's Theorem 90 for this case.
Solution. Let α be a root of $x^3 - 3x + 1$. We claim $\mathbb{Q}(\omega)(\alpha) = \mathbb{Q}(\omega, \alpha)$ is a splitting field of $x^3 - 3x + 1$ over $\mathbb{Q}(\omega)$. First observe since $x^3 - 3x + 1$ has no integral roots, $x^3 - 3x + 1$ is irreducible over $\mathbb{Q}$ by Gauss's Lemma (any factorization over $\mathbb{Q}$ would give a linear factor over $\mathbb{Z}$, and thus an integral root), and hence α has degree 3 over $\mathbb{Q}$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, α cannot lie in $\mathbb{Q}(\omega)$ and ω cannot lie in $\mathbb{Q}(\alpha)$, hence $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 3 \cdot 2$ and $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\omega)] = 3$. Next observe that the discriminant of $x^3 - 3x + 1$ is $-27 - 4 \cdot (-3)^3 = (-27) \cdot (1 - 4) = 81$, which is a perfect square, and hence $\mathbb{Q}(\omega, \alpha)$ is a splitting field of $x^3 - 3x + 1$ over $\mathbb{Q}(\omega)$. Since $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\omega)] = 3$, the Galois group G is cyclic of order 3. Let σ be a generator of G, and consider the Lagrange resolvant $\zeta = \alpha + \sigma(\alpha)\omega + \sigma^2(\alpha)\omega^2$. Then $\sigma(\zeta) = \sigma(\alpha) + \sigma^2(\alpha)\omega + \alpha\omega^2 = \omega^2\zeta$, so $\zeta \notin \mathbb{Q}(\omega)$ (since it is not fixed by σ) while $\zeta^3 \in \mathbb{Q}(\omega)$ (since $\sigma(\zeta^3) = (\sigma(\zeta))^3 = (\omega^2\zeta)^3 = \zeta^3$). The method developed in class shows (with appropriate sign choices) that ζ is a cube root of 27ω, so ζ is 3 times a primitive 9th root of 1.

Now write K as $\mathbb{Q}(\omega)[\zeta] = \mathbb{Q}(\omega) \oplus \mathbb{Q}(\omega)\zeta \oplus \mathbb{Q}(\omega)\zeta^2$. The generator σ of the Galois group may be chosen to send $\zeta \mapsto \zeta\omega$, so

$$\begin{aligned} N(x + y\zeta + z\zeta^2) &= (x + y\zeta + z\zeta^2)(x + y\zeta\omega + z\zeta^2\omega^2)(x + y\zeta\omega^2 + z\zeta^2\omega) \\ &= x^3 + 27\omega y^3 + 3^6\omega^2 z^3 - (81/2)xyz\omega. \end{aligned}$$

Thus the kernel of the norm map consists of those $x + y\zeta + z\zeta^2$, x, y, $z \in \mathbb{Q}(\omega)$, for which $x^3 + 27\omega y^3 + 3^6\omega^2 z^3 - (81/2)xyz\omega = 1$. Hilbert's Theorem 90 says this is the same as elements of the form

$$(x + y\zeta\omega + z\zeta^2\omega^2)/(x + y\zeta + z\zeta^2).$$

□