Solutions to Homework 6

Nathan Grigg

Section 7, Problems 1, 3, and 5

Exercise 1. Suppose that for some integer n, F contains the nth roots of unity, and K/F is a Galois extension of the form $K = F(\alpha)$, where $\alpha^n \in F$. What can you say about the Galois group $G = G(K/F)$?

Solution. We can say that $G(K/F)$ is cyclic. Note that α is a root of $f(x) = x^n - \alpha^n \in F[x]$. Let ω be a primitive nth root of unity; then $\alpha\omega^i$ is a root of $f(x)$ for each i between 0 and $n-1$. These numbers are all distinct, so these are all the roots of $f(x)$, which means that we have

$$f(x) = (x - \alpha)(x - \alpha\omega) \cdots (x - \alpha\omega^{n-1}).$$

Now, any F-automorphism of K is determined by where it sends α, and it must send roots of $f(x)$ to other roots of $f(x)$, so it is of the form $\sigma_i(\alpha) = \alpha\omega^i$ for some i. Note that $\sigma_i \circ \sigma_j = \sigma_{i+j}$, so there is a (clearly injective) homomorphism from G to C_n given by $\sigma_i \mapsto i$. Thus G is isomorphic to a subgroup of C_n, which means that G itself is also cyclic. □

Exercise 3. Let F be a subfield of $\mathbb{C}$ which contains i, and let K be a Galois extension of F whose Galois group is C_4. Is it true that K has the form $F(\alpha)$, where $\alpha^4 \in F$?

Solution. Yes. Let σ be a generator of $G(K/F)$. Then if β is an eigenvector of σ with eigenvalue λ, we have $\beta = \sigma^4(\beta) = \lambda^4\beta$. So $\lambda^4 = 1$.

Then since σ has finite order, it is diagonalizable, i.e., there is a basis for which the matrix for σ is diagonal whose entries are eigenvalues of σ. Suppose that $\pm i$ are not eigenvalues for σ, then the matrix for σ just has ± 1 down the diagonal, which means that σ^2 is the identity. This is a contradiction, so λ is an eigenvalue for σ for either $\lambda = i$ or $\lambda = -i$. Let γ be the corresponding eigenvector. Then

$$\gamma\sigma(\gamma)\sigma^2(\gamma)\sigma^3(\gamma) = \lambda\lambda^2\lambda^3\gamma^4 = -\gamma^4.$$

Since this is fixed by σ, it is in F, so $\gamma^4 \in F$. Also, $\sigma^k(\gamma) \neq \gamma$ for $k = 1, 2, 3$. Hence γ is not fixed by any subgroup of $\langle\sigma\rangle$, which implies that $K = F(\gamma)$. □

Exercise 5. Let K be a splitting field of an irreducible polynomial $f(x) \in F[x]$ of degree p whose Galois group is a cyclic group of order p generated by σ, and suppose that F contains the pth root of unity $\zeta = \zeta_p$. Show that there is an ordering $\alpha_1, \alpha_2, \ldots, \alpha_p$ of the roots of f such that

$$\beta = \alpha_1 + \zeta^{\nu}\alpha_2 + \zeta^{2\nu}\alpha_3 + \cdots + \zeta^{(p-1)\nu}\alpha_p$$

is an eigenvector of σ, with eigenvalue ζ^{-v}, unless it is zero.

Proof. Let α be a root of f and let $\alpha_i = \sigma^{i-1}(\alpha)$ for each i between 1 and p. Then we can write

$$\beta = \sum_{i=0}^{p-1} \zeta^{\nu i}\sigma^i(\alpha),$$

and we have

$$\sigma(\beta) = \sigma\left(\sum_{i=0}^{p-1} \zeta^{\nu i}\sigma^i(\alpha)\right) = \sum_{i=0}^{p-1} \zeta^{\nu i}\sigma^{i+1}(\alpha) = \sum_{j=1}^{p} \zeta^{-\nu}\zeta^{\nu j}\sigma^j(\alpha) = \zeta^{-\nu}\beta,$$

as desired. □