Comments on Problem Set 3

Math 250a

October 10, 2001

Problem 4. Write $F = k(s_1, \ldots, s_n)$. Let $f(X)$ be the polynomial $X^{2n} + \sum_{j=1}^{n} (-1)^j s_j X^{2(n-j)}$ of the problem. Then, in a splitting field L, we have the factorization

$$f(X) = (x - r_1)(x + r_1) \cdots (x - r_n)(x + r_n) \tag{1}$$

where the roots of f are $\pm r_j$, $1 \leq j \leq n$. Clearly $L = F(r_1, \ldots, r_n) = k(r_1, \ldots, r_n)$.

Multiplying out equation (1), we find that s_j is the j–th symmetric polynomial in $r_1^2, \ldots, r_n^2$. By an argument almost identical to Jacobson 4.15, the roots r_j in L are algebraically independent over F. Set $K := F(r_1^2, \ldots, r_n^2)$, so that $F \subset K \subset L$. Then K is the splitting field of $X^n + \sum_{j=1}^{n} (-1)^j s_j X^{n-j}$ over F, so by Jacobson 4.15, $\mathrm{Gal}(K/F) = S_n$.

We claim that $[L : K] = 2^n$. This is proved by adjoining the r_j's one at a time and observing that the degree goes up by a factor of 2 each time. For example, r_1 is not equal to any rational function in $r_1^2, \ldots, r_n^2$ because the r_j's are algebraically independent. Therefore $r_1 \notin K$, but $r_1^2 \in K$, so that $[K(r_1) : K] = 2$. Similarly $[K(r_1, r_2) : K(r_1)] = 2$, etc., and in the end

$$[L : K] = [K(r_1, \ldots, r_n) : K(r_1, \ldots, r_{n-1})] \cdots [K(r_1, r_2) : K(r_1)][K(r_1) : K] = 2^n.$$

Now let $\sigma \in \mathrm{Gal}(L/F)$. We know σ must permute the roots $\pm r_i$ in some fashion; the only question is which permutations are admissible for σ. Any automorphism must satisfy $\sigma(-r_j) = -\sigma(r_j)$, and one checks easily that there are exactly $2^n n!$ permutations of the set $\{\pm r_1, \pm r_2, \ldots, \pm r_n\}$ that satisfy $\sigma(-r_j) = -\sigma(r_j)$ for all j.[1]. Since every $\sigma \in \mathrm{Gal}(L/F)$ must have this form, we conclude that there are at most $2^n n!$ elements in $\mathrm{Gal}(L/F)$. But we also know that $[L : F] = [L : K][K : F] = 2^n n!$, so by the fundamental theorem of Galois theory, there are exactly $2^n n!$ elements in $\mathrm{Gal}(L/F)$, and it follows that every such permutation above corresponds to an element of $\mathrm{Gal}(L/F)$.

Therefore, the Galois group $\mathrm{Gal}(L/F)$ is the group of permutations σ of the set $\{\pm r_j\}$ satisfying $\sigma(-r_j) = -\sigma(r_j)$. This group is **not isomorphic** to $(\mathbf{Z}/2\mathbf{Z})^n \times S_n$—one easy way to see this is to take the case $n = 2$, where one can compute explicitly that the group is isomorphic to the nonabelian group D_4 and not to the abelian group $(\mathbf{Z}/2\mathbf{Z})^2 \times S_2$. One can also describe $\mathrm{Gal}(L/F)$ as the semidirect product $(\mathbf{Z}/2\mathbf{Z})^n \rtimes S_n$, where S_n acts on $(\mathbf{Z}/2\mathbf{Z})^n$ by permuting the factors.

Problem 6. See J. Rotman, *An Introduction to the Theory of Groups*, p. 113.

Problem 7. Let $\zeta := e^{2\pi i/p}$ be a primitive p–th root of unity. Then the roots of $x^p - c$ are $\zeta^j \sqrt[p]{c}$, for $0 \leq j \leq p-1$. The splitting field K of $x^p - c$ is then $\mathbf{Q}(\sqrt[p]{c}, \zeta\sqrt[p]{c}, \ldots, \zeta^{p-1}\sqrt[p]{c}) = \mathbf{Q}(\zeta, \sqrt[p]{c})$.

We claim $[K : \mathbf{Q}] = p(p-1)$. From class we know that the minimal polynomial for ζ over $\mathbf{Q}$ is $(x^p - 1)/(x - 1)$, so $[\mathbf{Q}(\zeta) : \mathbf{Q}] = p - 1$. We are given that $x^p - c$ is irreducible over $\mathbf{Q}$, so $[\mathbf{Q}(\sqrt[p]{c}) : \mathbf{Q}] = p$. Since K contains both $\mathbf{Q}(\zeta)$ and $\mathbf{Q}(\sqrt[p]{c})$, the degree $[K : \mathbf{Q}]$ is at least as big as the LCM of p and $p - 1$, which is $p(p-1)$. On the other hand, $\sqrt[p]{c}$ has degree at most p over $\mathbf{Q}(\zeta)$ (since it satisfies the polynomial equation $x^p - c = 0$ over $\mathbf{Q}(\zeta)$), so

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(\zeta)][\mathbf{Q}(\zeta) : \mathbf{Q}] \leq p(p-1).$$

[1] Explicitly, they are given as follows: there are $n!$ ways to permute $\{r_j\}$, and given such a permutation there are 2^n ways to assign $+$ signs or $-$ signs to the values of the r_j's

Therefore $[K : \mathbf{Q}] = p(p-1)$.

Any element σ of $\mathrm{Gal}(K/\mathbf{Q})$ must map $\sqrt[p]{c}$ to another root of $x^p - c$, and ζ to another root of $(x^p - 1)/(x - 1)$. Also, σ is determined by its action on these two elements. There are p choices in the first case and $p - 1$ choices in the second case, so there are at most $p(p-1)$ possibilities for σ. But we know $[K : \mathbf{Q}] = p(p-1)$, so each of these possibilities must actually occur. If we make the choice $\sigma(\sqrt[p]{c}) = \zeta^b \sqrt[p]{c}$, and $\sigma(\zeta) = \zeta^a$, then

$$\sigma(\zeta^x \sqrt[p]{c}) = \zeta^{ax+b} \sqrt[p]{c}. \quad (1 \leq a \leq p-1, \quad 0 \leq b \leq p-1) \tag{2}$$

The isomorphism from $\mathrm{Gal}(K/\mathbf{Q})$ to the "$ax + b$ group mod p" is given by identifying $\mathbf{Z}/p\mathbf{Z}$ with the multiplicative group $G = \{1, \zeta, \zeta^2, \ldots, \zeta_{p-1}\}$. By (2), the element σ induces an action on G exactly equal to the "$ax + b$ group" action on $\mathbf{Z}/p\mathbf{Z}$, and by the previous paragraph, all possibilities for a and b actually occur in $\mathrm{Gal}(K/\mathbf{Q})$.