Math 250A, Fall 2004
Homework Assignment #9
Last assignment, due December 9, 2004

Prove Corollary 1.4 on page 263.

In the Galois correspondence between subgroups of $\mathrm{Gal}(K/k)$ and fields between k and K, let I be the subgroup of $\mathrm{Gal}(K/k)$ that corresponds to $F \cap F'$. Then I contains both H and H' because $F \cap F'$ is contained in both F and F'. In the other direction, suppose that J is a subgroup of $\mathrm{Gal}(K/k)$ that contains both H and H'. Then the field corresponding to J is contained in both F and F' and is therefore in the intersection $F \cap F'$. Accordingly, J contains I. Therefore I is the smallest subgroup of $\mathrm{Gal}(K/k)$ that contains H and H: it's contained in any such subgroup. Moral: this problem really is "obvious" once you understand the correspondence between fields and groups.

Problems from Chapter VI: 1 (a–e), 5, 6, 7, 9, 11, 15.

1. Part (a): The polynomial $x^3 - x - 1$ is irreducible over $\mathbf{Q}$ for various reasons. The simplest way to see that it's irreducible is to use the Integral Root Test on page 185 and to observe that ± 1 are not roots. The Galois group is then either $\mathbf{A}_3$, the cyclic group of order 3, or the symmetric group $\mathbf{S}_3$. To decide between the two alternatives, we compute the discriminant of the polynomial. (All this is on page 270.) Here, the discriminant is -23, which is a non-square. Thus the Galois group is $\mathbf{S}_3$.

Part (b): By Eisenstein's criterion for the prime 2, $x^3 - 10$ is irreducible over $\mathbf{Q}$. The splitting field of the polynomial contains the field of cube roots of 1, which is the quadratic field $\mathbf{Q}(\sqrt{-3})$. Thus the Galois group has order divisible by 2. Since we know (as in part a) that the Galois group is either $\mathbf{A}_3$ or $\mathbf{S}_3$, we conclude that it must be $\mathbf{S}_3$, as in the previous part. Note, for the next part, that the splitting field of $x^3 - 10$ has a *unique* quadratic subfield; this follows, via the Galois correspondence, from the fact that $\mathbf{S}_3$ has a unique subgroup of index 3. The unique quadratic subfield of the splitting field is then the one that we know about, namely $\mathbf{Q}(\sqrt{-3})$.

Part (c): Let K_1 be the splitting field of $x^3 - 10$ and let K_2 be the splitting field of $x^2 - 2$; thus $K_2 = \mathbf{Q}(\sqrt{2})$. By the discussion at the end of the previous part, we know that $K_1 \cap K_2 = \mathbf{Q}$. In Theorem 1.14 on page 267, take $k = \mathbf{Q}$. The Galois group of $K_1 K_2$ over $\mathbf{Q}$ is then seen to be $\mathbf{S}_3 \times \mathbf{Z}/2\mathbf{Z}$, a group of order 12. The Galois group of $K_1 K_2$ over K_2, which is what we want to calculate, is the same group as the Galois group of K_1 over $K_1 \cap K_2 = \mathbf{Q}$, which was $\mathbf{S}_3$.

Part (d): In view of all of our discussion above, I hope that you will see that the answer here is $\mathbf{A}_3$.

Part (e): A blast from the past: we're back to part (a). The field $\mathbf{Q}(\sqrt{-23})$ is the discriminant field: the splitting field of $x^3 - x - 1$ contains $\mathbf{Q}(\sqrt{-23})$ because the discriminant of the polynomial is -23. Thus we are in the same situation as in part (d), which is to say that the Galois group is once again $\mathbf{A}_3$.

5. The first part is a fairly straightforward abstraction of what we saw already in exercises 1c and 1e. Namely, let K_1 be the splitting field of f and let K_2 be the splitting field of g.

Things are set up so that the K_i are Galois over k and so that the Galois groups of K_1/k and K_2/k are $\mathbf{S}_3$ and $\mathbf{Z}/2\mathbf{Z}$, respectively. Further, the assumption $k(\sqrt{D}) \neq k(\sqrt{c})$ means that K_2 is not contained in K_1. Accordingly, $K_1 \cap K_2 = k$. We know from Theorem 1.14 that the Galois group of K_1K_2 over k is the product of the two groups $\mathbf{S}_3$ and $\mathbf{Z}/2\mathbf{Z}$; this product has order 12.

For the second part, we view the degree $[k(\gamma) : k]$ as the number of conjugates of $\gamma = \alpha+\beta$ over k. The conjugates of γ are simply the images $\sigma(\gamma)$ as σ runs over the Galois group of K_1K_2/k. The number α has 3 conjugates, while the number β has two conjugates; thus, γ has at most 6 conjugates. The point, however, is that $\mathrm{Gal}(K_1K_2/k)$ is the product of $\mathrm{Gal}(K_1/k)$ and $\mathrm{Gal}(K_2/k)$, by Theorem 1.14. This means, concretely: if you have a conjugate $\sigma_1(\alpha)$ with $\sigma_1 \in \mathrm{Gal}(K_1/k)$ and a conjugate $\sigma_2(\beta)$ with $\sigma_2 \in \mathrm{Gal}(K_2/k)$, there is a $\sigma \in \mathrm{Gal}(K_1K_2/k)$ that induces σ_1 on K_1 and σ_2 on K_2. We then have $\sigma(\gamma) = \sigma_1(\alpha) + \sigma_2(\beta)$. There are 3 choices for the first term and 2 for the second; thus there are 6 choices for the sum.

6. In the first part, K/E is a quadratic extension, with $\mathrm{Gal}(K/E)$ being generated by σ^2. We have set things up in the usual way: $K = E(\sqrt{\gamma})$ with $\gamma \in E$. Thus the non-trivial conjugation σ^2 sends $\sqrt{\gamma}$ to $-\sqrt{\gamma}$. We have given a name to a specific square root of γ in K: this is α. Let $z = \dfrac{\sigma\alpha}{\alpha}$. Then certainly $z^2 = \dfrac{\sigma(\alpha^2)}{\alpha^2} = \dfrac{\sigma\gamma}{\gamma}$. Also $z \cdot \sigma(z) = \dfrac{\sigma\alpha}{\alpha}\dfrac{\sigma^2(\alpha)}{\sigma\alpha} = \dfrac{\sigma^2(\alpha)}{\alpha} = -1$ because σ^2 takes $\alpha = \sqrt{\gamma}$ to its negative. Since σ sends z to its negative reciprocal, σ^2 sends z back to z. Thus z is fixed by σ^2, so it lies in E.

In the second part, we have only E/k, and there's a τ playing the role of σ^2. The element z such that $\tau : z \mapsto -1/z$ is given to us. Note that τ sends z^2 to $1/z^2$. We prove that $z^2 \neq -1$: if $z^2 = -1$, then z and τz are the two roots of $X^2 + 1 = 0$, so their product is 1, not -1. (Note that 1 and -1 are distinct because the characteristic is not 2.) We take $\gamma = \dfrac{1}{1+z^2}$; then $\tau\gamma/\gamma = z^2$, as required. We continue by letting α be a square root of γ. As in the statement of the problem, put $K = k(\alpha)$ and let σ be an extension of τ to a map $K \to \overline{K}$. (Note that K contains E because E is generated over k by α^2.) Observe that $\sigma(\alpha^2) = \sigma(\gamma) = z^2\gamma = z^2\alpha^2$. Thus $\dfrac{\sigma\alpha}{z\alpha}$ has square 1, so that $\sigma\alpha = \pm z\alpha$. Prompted by the book, we change the sign of z if necessary to have $\sigma\alpha = z\alpha$. Since z is in E, z is in K, so that σ maps α back to K. Thus σ is an automorphism of K. Using the equation $\sigma\alpha = z\alpha$, we get $\sigma^2(\alpha) = \sigma(z)\sigma(\alpha) = -\alpha$, and then $\sigma^4(\alpha) = 1$. Thus σ has order divisible by 4. Since K/k has degree 4, σ must be exactly of order 4, and K/k is seen now to be a cyclic extension of degree 4. I think that we've done the whole problem now.

7. For part a, assume that we have $K \hookrightarrow L$, where $L/\mathbf{Q}$ is cyclic of degree $2n$, with n even. Without loss of generality, we can and will suppose that L is a subfield of $\mathbf{C}$. Let τ be the restriction to L of the complex conjugation map $\mathbf{C} \to \mathbf{C}$, and let σ be a generator of $\mathrm{Gal}(L/\mathbf{Q})$. We must have $\tau = \sigma^n$ because σ^n is the unique element of $\mathrm{Gal}(L/\mathbf{Q})$ of order 2. Note now that the restrictions to K of both τ and σ are of order 2: τ gives a non-trivial automorphism of K because $\sqrt{a}$ is imaginary, while σ gives a non-trivial automorphism of K because the fixed field of σ is $\mathbf{Q}$. If $\alpha = \sqrt{a}$, then $\sigma(\alpha) = \tau(\alpha) = -\alpha$.

On the other hand, the formula $\tau = \sigma^n$ shows that $\tau\alpha = (-1)^n\alpha$. Since n is even, we have a contradiction.

For part b, we can use the analysis of problem 6. Start with $E = \mathbf{Q}(\sqrt{5})$, and let τ be the non-trivial conjugation of E over $\mathbf{Q}$. Let $z = 2 - \sqrt{5}$. Then $z\tau z = (2-\sqrt{5})(2+\sqrt{5}) = 4 - 5 = -1$. If $\gamma = 15 + 6\sqrt{5}$, then $\dfrac{\tau\gamma}{\gamma} = z^2$ (I hope). If α is a square root of γ, then $\mathbf{Q}(\alpha)$ if cyclic of degree 4 over $\mathbf{Q}$. Note that γ satisfies $t^2 - 30t + (225 - 180) = 0$ or $t^2 - 30t + 45 = 0$ and α satisfies $x^4 - 30x^2 + 45 = 0$, which is the polynomial we want, except for a sign. It looks like I should have taken $\gamma = -15 + 6\sqrt{5}$; make the appropriate changes. . . .

Part c, now. This is similar; start with $z = \sqrt{2} - 1$ in $E = \mathbf{Q}(\sqrt{2})$.

9. For each i, there is an isomorphism $k(\theta) \xrightarrow{\sim} k(\theta_i)$ that we know about: it takes a polynomial $g(\theta)$ in θ with coefficients in k to the number $k(\theta_i)$. By hypothesis, if $i = 2$ we get an *automorphism* σ of $K = k(\theta)$. This automorphism is non-trivial since it does not fix θ. Let G be the subgroup of $\mathrm{Aut}_k K$ that is generated by σ, and let E be the fixed field of G. We have $k \subseteq E \subseteq K$. By Artin's theorem, K/E is a Galois extension with group G. Since G is non-trivial, E is smaller than K. By the tower law (since $[K : k]$ is prime), we have $E = k$. Thus K/k is Galois. Its Galois group is cyclic: it's the cyclic group generated by σ.

11. Our situation is that k is a subfield of $\mathbf{R}$ and that we are looking at roots of f in $\mathbf{C}$. We let $^-$ be the complex conjugation map on $\mathbf{C}$. We suppose that there is a root α such that $\bar{\alpha} \neq \alpha$ and such that $\alpha\bar{\alpha} = 1$. Note that $\bar{\alpha}$ is again a root of f because k is in $\mathbf{R}$. Thus α is a root of f such that $1/\alpha$ is also a root of f. All roots of f are of the form $\sigma\alpha$, where σ is an automorphism of the splitting field of f over k. We have $f(1/\sigma(\alpha)) = \sigma(f(1/\alpha)) = \sigma(0) = 0$, so that $1/\sigma(\alpha)$ is a root of f. Thus the reciprocal of each root of f is again a root of f. It is easy now to see that f has even degree. Indeed, the map $\alpha \mapsto 1/\alpha$ is an involution on the set of roots of f. This involution has no fixed points—the fixed points would be ± 1, numbers that are not roots of f because f is irreducible with a non-real root.

15. Let H for us be $\mathrm{Gal}(K/F)$ and let N be the group that Lang calls H: the group of all $g \in \mathrm{Gal}(K/k)$ such that $gF = F$. Note that $gHg^{-1} = H$ if and only if H and gHg^{-1} have the same fixed field. The fixed field of H is F while the fixed field of gHg^{-1} is gF, as we saw in class last week. Hence g belongs to N if and only if $gHg^{-1} = H$, i.e., if and only if g normalizes H.