Math 250A, Fall 2004
Homework Assignment #9
Problems due November 30, 2004

Problems from Lang's Chapter V:

**3.** In this context, $\alpha$ and $\beta$ lie in some field containing $F$; call this field $E$ if you want. Then $[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\alpha)][F(\alpha):F] = [F(\alpha,\beta):F(\beta)][F(\beta):F]$ by the tower law. Thus $[F(\alpha,\beta):F]$ is divisible both by $[F(\alpha):F]$ and by $[F(\beta):F]$. Since these numbers are relatively prime, $[F(\alpha,\beta):F]$ is divisible by their product, $[F(\alpha):F][F(\beta):F]$. Accordingly, $[F(\alpha,\beta):F(\alpha)]$ is divisible by $[F(\beta):F]$. Now the degree $[L(\beta):L]$ is the degree of the irreducible polynomial of $\beta$ over $L$; we apply this remark with $L = F$ and $L = F(\alpha)$. We conclude that the degree of irreducible polynomial of $\beta$ over $F(\alpha)$ is divisible by the degree of the irreducible polynomial of $\beta$ over $F$. Since the former polynomial divides the latter, the two polynomials must be equal. This means that the irreducible polynomial of $\beta$ over $F$ remains irreducible over $F(\alpha)$, which is what we were required to show.

**5.** We know a lot more than typical readers of this problem, since we have discussed in class the material on page 278. The first thing that we should point out is that $x^6+x^3+1$ is irreducible. If you call this polynomial $f(x)$, then $f(x+1) = x^6+6x^5+15x^4+21x^3+18x^2+9x+3$ is Eisenstein at 3. In general, if $\alpha$ is an algebraic number, the maps $\mathbf{Q}(\alpha) \to \mathbf{C}$ correspond to roots $\beta$ of the minimal polynomial of $\alpha$. Given $\beta$, you get a map by sending $g(\alpha)$ to $g(\beta)$; here $g$ is a polynomial with rational coefficients. (See p. 233.) The main point of this problem is to characterize the various possible $\beta$'s in our situation. Note that $f(x)(x^3-1) = x^9-1$. This shows that every root of $f(x)$ is a primitive 9th root of unity. There are six primitive 9th roots of unity, and the irreducibility of $f(x)$ amounts to the statement that all primitive 9th roots of unity are roots of $f(x)$. The primitive 9th roots of unity are the $\alpha^i$ with $i$ prime to 3 (and taken mod 9). Thus the embeddings $\mathbf{Q}(\alpha) \to \mathbf{C}$ are the maps $g(\alpha) \mapsto g(\alpha^i)$ with $i = 1,2,4,5,7,8$.

**7.** We have $[EF:k] = [EF:F][F:k]$ so that the inequality $[EF:k] \le [E:k][F:k]$ is equivalent to the inequality $[EF:F] \le [E:k]$. If $E = k(\alpha)$, then $EF = F(\alpha)$, and we get the desired inequality by noting that the degree of the minimal polynomial of $\alpha$ over $F$ is no bigger than the corresponding degree over $k$. (As noted in the discussion of problem 3, the minimal polynomial over $F$ divides the minimal polynomial over $k$.) We prove the sought-after inequality in general by writing $E = k(\alpha_1,\ldots,\alpha_t)$ and doing an induction on $t$. (I won't write the details.) The final assertion about relatively prime degrees runs as in problem 3: We observe that $[EF:k]$ is divisibly by both $[E:k]$ and $[F:k]$ and is thus divisible by the product of these indices.

**9.** We have $x^{p^8}-1 = (x-1)^{p^8}$ over the field $\mathbf{Z}/p\mathbf{Z}$ because of the general formula $(a+b)^p = a^p+b^p$ in characteristic $p$. Hence the polynomial $x^{p^8}-1$ splits completely already over $\mathbf{Z}/p\mathbf{Z}$; its splitting field is the prime field $\mathbf{Z}/p\mathbf{Z}$!

**11.** OK, so we have a large bunch of splitting fields to figure out:

$x^2 - 2$

The splitting field is $\mathbf{Q}(\sqrt{2})$. The degree of the field is 2. We know this because $x^2 - 2$ is irreducible (it's Eisenstein at 2) and splits completely once we have one root.

$x^2 - 1$

The splitting field is $\mathbf{Q}$. The polynomial splits as $(x-1)(x+1)$.

$x^3 - 2$

This problem is analogous to the last problem (with $x^5 - 7$), which I typed before this one. The splitting field has degree 6 over $\mathbf{Q}$. Thus 6 is the new 20 if you do the problems in reverse order. Otherwise, 20 is the new 6.

$(x^3 - 2)(x^2 - 2)$

The splitting field is $\mathbf{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{2})$, which we view as the composite $EF$, where $E = \mathbf{Q}(\sqrt{2}, \sqrt{-3})$ and $F = \mathbf{Q}(\sqrt[3]{2})$. The degree $[E : \mathbf{Q}]$ is 4, as we can see in various ways; note, for example, that $\mathbf{Q}(\sqrt{2}, \sqrt{-3})/\mathbf{Q}(\sqrt{2})$ has to be a quadratic extension because the field $\mathbf{Q}(\sqrt{2}) \subseteq \mathbf{R}$ cannot contain a square root of $-3$. The degree of $F$ over $\mathbf{Q}$ is 3, as was implicit in our brief discussion of the previous polynomial. By problem 7, the degree of the splitting field over $\mathbf{Q}$ is 12.

$x^2 + x + 1$

This is like the first polynomial. The splitting field is $\mathbf{Q}(\sqrt{-3})$, as we see from the quadratic formula (or by completing the square).

$x^6 + x^3 + 1$

As we saw in problem 5, the polynomial is irreducible. If $\alpha$ is one root, then the other roots are powers of $\alpha$. Thus the splitting field is $\mathbf{Q}(\alpha)$, where $\alpha$ is a root. This field has degree 6 over $\mathbf{Q}$.

$x^5 - 7$

The polynomial is irreducible (Eisenstein at 7). If $\alpha$ is one root (for example, the real fifth root of $7 \approx 1.47577$) and $\beta$ is a primitive fifth root of 1 (for example $e^{\frac{2\pi i}{5}}$), then the splitting field is clearly $\mathbf{Q}(\alpha, \beta)$. Indeed, the roots of the polynomial are the numbers $\alpha\beta^j$ with $j = 0, \ldots 4$. The field $\mathbf{Q}(\alpha)$ has degree 5 over $\mathbf{Q}$, while $\mathbf{Q}(\beta)$ has degree 4 over $\mathbf{Q}$; note that the minimal polynomial of $\beta$ is $x^4 + x^3 + x^2 + x + 1$. The splitting field $\mathbf{Q}(\alpha, \beta)$ has degree 20 over $\mathbf{Q}$ because 4 and 5 are relatively prime. A good exercise for December is to describe the Galois group $\operatorname{Gal}(\mathbf{Q}(\alpha, \beta)/\mathbf{Q})$. Alumni of Math 114 from last semester should be able to do this with ease (right?).