Math 250A | Professor K. A. Ribet
Final Exam | December 13, 2001

Question 0 was worth for 0 points. The other questions will count for 6 points each. The maximum possible score on this exam will be 42.

0. *Name a French mathematician who died as the result of a duel.*

I asked this question once before, on an exam for our undergraduate Galois theory course (Math 114). When I asked the question, I misspelled "duel" as "dual"; some of the students made fun of me for this. Also, I worded the question in such a way that I had Galois dying at the duel. However, I was told today at the MSRI that he died the next day as a result of wounds that he got at the duel.

1. *Let A be a normal subgroup of order p of a finite p-group G. Prove that A is contained in the center of G.*

The group G acts on A by conjugation via a homomorphism $G\colon \operatorname{Aut} A$. The target group has order $p-1$, while the source group has p-power order. Thus the homomorphism is trivial—everything in G is mapped to the identity automorphism. Thus A is in the center of G, as required.

2. *In a non-abelian group of order 55, find the number of elements of order n for $n = 1$, 5, 11, 55. Are there non-abelian groups of order 55?*

There are no elements of order 55; if there were, the group would be cyclic, hence abelian. There is one element of order 1: the identity. There is precisely one 11-Sylow subgroup of the group because the number of 11-Sylows divides 5 and is congruent to 1 mod 11. Hence there are 10 elements of order 11. It follows that the number of elements of order 5 is $55 - 1 - 10 = 44$. This statement is equivalent to the fact that there are 11 5-Sylow subgroups of the group, which we could have seen otherwise. To construct a non-abelian group of order 55, we should take a semi-direct product. The idea is that a group of order 5 can act non-trivially on a group of order 11 since the group of automorphisms of a group of order 11 has order 10 and thus has some elements of order 5. A good exercise, which I haven't done, is to calculate the number of non-abelian groups of order 55, up to isomorphism.

3. *Let $\mathbf{F}$ be a finite field, and set $q = \#(F)$. For each $d \geq 1$, let $f_d \in \mathbf{F}[X]$ be the product of the monic irreducible degree-d polynomials over $\mathbf{F}$. Show, for each $n \geq 1$, that $X^{q^n} - X = \prod_{d|n} f_d$.*

I haven't yet graded this question yet; in fact, I'm about to grade it. I anticipate that there will be some question about what information it's legitimate to use in your solution. What's clear to me going in is that the polynomial $X^{q^n} - X$ has derivative -1; hence, it cannot be divisible by the square of any non-constant polynomial. Accordingly, when we factor it as a product of irreducible polynomials, each polynomial in the product occurs only once. Thus it suffices to show that an irreducible polynomial $f(x)$ divides $X^{q^n} - X$ if and only if its degree divides n. Let $\overline{\mathbf{F}}$ be an algebraic closure of $\mathbf{F}$. As explained on page 245 of our text, the roots of $X^{q^n} - X$ in $\overline{\mathbf{F}}$ form a field $\mathbf{F}'$ of degree n over $\mathbf{F}$. (Thus $\mathbf{F}'$ has q^n elements.) Suppose that $f(x)$ is an irreducible polynomial that divides $X^{q^n} - X$, and let α be a root of $f(x)$ in $\overline{\mathbf{F}}$. Then $\alpha \in \mathbf{F}'$, which implies that $\mathbf{F}(\alpha)$ is a subfield of $\mathbf{F}'$. Hence $[\mathbf{F}(\alpha) : \mathbf{F}]$ divides n. Since this field degree is the degree of f, we get that the degree of f divides n. Conversely, suppose that d, the degree of f, divides n and let α be a root of f in $\overline{\mathbf{F}}$. Since $\mathbf{F}(\alpha)$ has degree d over $\mathbf{F}$, all elements of $\mathbf{F}(\alpha)$ satisfy $X^{q^d} - X$. In particular, α satisfies this polynomial, which implies that $f(X) = \mathrm{Irr}(\alpha, \mathbf{F}, X)$ divides $X^{q^d} - X$. This latter polynomial is a divisor of $X^{q^n} - X$.

4. *Let K/k be a finite Galois extension. Set $G = \mathrm{Gal}(K/k)$ and let H be a subgroup of G. Express the group of field automorphisms $\mathrm{Aut}_k(K^H)$ as a quotient of a subgroup of G.*

Let $F = K^H$. An automorphism of F is the restriction to F of an automorphism of K. (Maps $F \to K$ can be extended to maps $K \to \overline{K}$, but these latter extensions have images in K.) Let g be an automorphism of K (tacitly assumed to be the identity on k). Then g maps F, which corresponds to the subgroup H of G, to the field gF, which corresponds to gHg^{-1} under the Galois correspondence. We thus have $gF = F$ if and only if $gHg^{-1} = H$, i.e., if and only if $g \in N(H)$, where $N(H)$ is the normalizer of H. Thus $\mathrm{Aut}_k(F)$ is a quotient of $N(H)$. A g acts as the identity on F if and only if g belongs to H. Hence $\mathrm{Aut}_k(F) = N(H)/H$.

5. *Let p be a prime number different from 2, and let ζ be a complex pth root of 1 ($\zeta \neq 1$). Set $\alpha = \zeta + \zeta^{-1}$. Show that $\mathbf{Q}(\alpha)$ is a Galois extension of $\mathbf{Q}$ and determine the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$. When $p = 7$, calculate $\mathrm{Irr}(\alpha, \mathbf{Q}, X)$.*

As we discussed in class, $\mathbf{Q}(\zeta)$ is a Galois extension of $\mathbf{Q}$ whose degree is $p - 1$. The Galois group of the extension is canonically $(\mathbf{Z}/p\mathbf{Z})^*$, a cyclic group of order $p - 1$. In the dictionary between elements of $(\mathbf{Z}/p\mathbf{Z})^*$ and automorphisms of $\mathbf{Q}(\zeta)$, the number i mod p corresponds to the automorphism that sends ζ to ζ^i. Since $\mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\zeta)$, $\mathbf{Q}(\alpha)$ is a cyclic extension of $\mathbf{Q}$ of degree dividing $p - 1$. The degree is the number of distinct conjugates $alpha_i := \zeta^i + \zeta^{-i}$ of $\alpha = \zeta + \zeta^{-1}$. Let us calculate the number of distinct α_i. Certainly α_i depends only on the image of i in $(\mathbf{Z}/p\mathbf{Z})^*/\{\pm 1\}$; i.e., $\alpha_i = \alpha_{-i}$. Conversely, suppose $\alpha_i = \alpha_j$, which is to say that $\zeta^i + \zeta^{-i} = \zeta^j + \zeta^{-j}$. We can suppose that we have $1 \leq i, j \leq p-1$ for definitiveness. An important fact here is that the numbers $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ are linearly independent over $\mathbf{Q}$. Indeed, a linear dependence among them would yield on division by ζ a linear dependence among $1, \zeta, \ldots, \zeta^{p-2}$, which would contradict the fact that ζ has degree $p - 1$ over $\mathbf{Q}$. The important fact implies that $i = \pm j$, which is enough to show that there are $(p - 1)/2$ different α_i. Hence $\mathbf{Q}(\alpha)$ has degree $(p - 1)/2$ over $\mathbf{Q}$.

To find the minimal polynomial of α for $p = 7$ is a computation that is either annoying or amusing, depending on your mood and personality. I did the computation in preparation for a lecture last month, but I didn't have time to present it in my lecture. The idea is to start with the minimal polynominal for ζ and to divide it by the middle power of ζ so that ζ and ζ^{-1} occur in a balanced way:

$$0 = \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 \implies 0 = (\zeta^3 + \zeta^{-3}) + (\zeta^2 + \zeta^{-2}) + (\zeta + \zeta^{-1}) + 1.$$

We have to write each of the terms in parentheses on the right-hand side as a polynomial in $\alpha = \zeta + \zeta^{-1}$. Since $\alpha^2 = \zeta^2 + 2 + \zeta^{-1}$, $\zeta^2 + \zeta^{-2} = \alpha^2 - 2$. Also $\alpha^3 = \zeta^3 + 3(\zeta + \zeta^{-1}) + \zeta^{-3}$, so $\zeta^3 + \zeta^{-3} = \alpha^3 - 3\alpha$. Thus

$$0 = \alpha^3 - 3\alpha + \alpha^2 - 2 + \alpha + 1 = \alpha^3 + \alpha^2 - 2\alpha - 1.$$

Your mileage here may vary—I may have screwed up this computation, which I'm doing directly onto the screen. On the other hand, I just used a computer algebra system to compute the discriminant of $x^3 + x^2 - 2x - 1$; the discriminant is 49, so I'm actually now fairly confident that I got the right answer.

6. *Let S be a multiplicative subset of a commutative ring A. Let $\mathcal{I}$ be the set of ideals of A that contain no element of S. Show that each maximal element of $\mathcal{I}$ is a prime ideal of A.*

This was a homework problem, I believe. I believe also that I sketched or wrote out a solution based on the correspondence between ideals of A and ideals of $S^{-1}A$. Let's try to do this directly. Take a maximal element $I \in \mathcal{I}$ and suppose that it's not prime. Then there are $x, y \in A$ with $x \notin I$, $y \notin I$, but $xy \in I$. The ideal $(x) + I$ is bigger than I so must contain an element s of S. Similarly, $(y) + I$ contains some $s' \in S$. Thus the ideal $J := \big((x) + I\big)\big((y) + I\big)$ contains $ss' \in S$. However, it is clear that we have $J \subseteq I$ because $xy \in I$.

7. *Suppose that A is an abelian group with the following extension property: If N is a subgroup of an abelian group M and $\varphi\colon N \to A$ is a homomorphism, there is a homomorphism $\Phi\colon M \to A$ that extends φ. Show that A is a* divisible *abelian group: for each $a \in A$ and $n \geq 1$, there is a b in A so that $nb = a$.*

Given $a \in A$, we define $\varphi\colon \mathbf{Z} \to A$ so that $1 \mapsto a$. We consider $\mathbf{Z}$ as a subgroup of $\mathbf{Q}$ (the additive group of rationals) and choose $\Phi\colon \mathbf{Q} \to A$ extending φ. We can take $b = \Phi\dfrac{1}{n}$; then $nb = a$.