Final Exam – 05/21/08

Instructor: T. Haines
Math 601

In your exam book, CLEARLY LABEL each problem by number and part. SHOW ALL WORK.

Each problem is worth 20 points. Solve 6 problems. Total points: 120.

1. (a) Let p be a prime number. Suppose $X^p - p = \prod_{i=1}^{p} X - \alpha_i$, for $\alpha_i \in \overline{\mathbb{Q}}$. Find $[\mathbb{Q}(\alpha_1, \ldots, \alpha_p) : \mathbb{Q}]$.

ANSWER: The field $\mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ is the splitting field of $X^p - p$, and we want to find its degree over $\mathbb{Q}$. We have $\mathbb{Q}(\alpha_1, \ldots, \alpha_p) = \mathbb{Q}(p^{1/p}, \xi)$ where ξ denotes a primitive p-th root of unity. By Eisenstein $X^p - p$ is irreducible over $\mathbb{Q}$, so that $[\mathbb{Q}(p^{1/p}) : \mathbb{Q}] = p$. Also, we know ξ has degree $p-1$ over $\mathbb{Q}$ (the p-th cyclotomic polynomial has degree $p-1$). Since $(p, p-1) = 1$, our splitting field, the compositum $\mathbb{Q}(p^{1/p})\mathbb{Q}(\xi)$, has degree $p(p-1)$ over $\mathbb{Q}$.

(b) What is the degree over $\mathbb{Q}$ of the splitting field of $X^6 - 3$?

ANSWER: *First Proof:* First, the above shows that the splitting field of $Y^3 - 3$ has degree 6 over $\mathbb{Q}$, and since this is strictly smaller than the splitting field of $X^6 - 3$, the latter has degree at least 12 over $\mathbb{Q}$. On the other hand, $X^6 - 3$ is split by adjoining $3^{1/6}$ and ξ_6 (a primitive 6-th root of unity) to $\mathbb{Q}$, and $[\mathbb{Q}(3^{1/6}) : \mathbb{Q}] = 6$ (Eisenstein) and $[\mathbb{Q}(\xi_6) : \mathbb{Q}] = \phi(6) = 2$, hence the degree of the splitting field of $X^6 - 3$ has degree at most $6 \cdot 2 = 12$. So the degree is exactly 12.

Second Proof: $X^6 - 1 = (X-1)(X^2 + X + 1)(X+1)(X^2 - X + 1)$, from which it follows that $\mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(i\sqrt{3})$. So, the splitting field $\mathbb{Q}(3^{1/6}, \xi_6) = \mathbb{Q}(3^{1/6}, i)$. Since i is not real, i has degree 2 over $\mathbb{Q}(3^{1/6})$, which in turn has degree 6 over $\mathbb{Q}$ (Eisenstein). Hence by multiplicativity of degrees, we get $[\mathbb{Q}(3^{1/6}, i) : \mathbb{Q}] = 12$.

2. (a) Let $\xi = e^{2\pi i/7}$. Verify that the minimum polynomial for $\xi + \xi^{-1}$ over $\mathbb{Q}$ is $X^3 + X^2 - 2X - 1$.

ANSWER: Since $\xi^7 = 1$ and $\xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$, the verification that $\xi + \xi^{-1}$ satisfies $X^3 + X^2 - 2X - 1$ follows easily on noting that

$$\begin{aligned}(\xi + \xi^{-1})^3 &= \xi^3 + 3\xi + 3\xi^{-1} + \xi^{-3} = \xi^3 + 3\xi + 3\xi^6 + \xi^4 \\ (\xi + \xi^{-1})^2 &= \xi^2 + 2 + \xi^{-2} = \xi^2 + 2 + \xi^5 \\ \xi + \xi^{-1} &= \xi + \xi^6.\end{aligned}$$

Why is this the *minimum* polynomial? If $\xi + \xi^{-1}$ satisfies a polynomial of form $aX^2 + bX + c$, then by using the above computations we'd get that ξ satifies a polynomial of degree at most 6, which is *different* from the 7th cyclotomic polynomial (it can't have any degree 3 or 4 terms). But then subtracting we'd get that ξ would have degree strictly lower than 6, a contradiction.

(b) Find the Galois group of $X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

ANSWER: *First proof.* Let $f := X^3 + X^2 - 2X - 1$; it is irreducible, being a minimum polynomial and so 3 divides the degree of its splitting field, i.e. $3||G(f)|$. The degree of the splitting field is at most $3! = 6$, and so $|G(f)| \leq 6$. Moreover $\xi + \xi^{-1} = 2\cos(2\pi/7)$ is real, so f has at least one real root. If it had exactly one real root, then $G(f) \cong S_3$ (by a Homework problem). The splitting field is contained in $\mathbb{Q}(\xi)$, which is Galois over $\mathbb{Q}$ with Galois group the abelian group $(\mathbb{Z}/7\mathbb{Z})^\times$. Therefore $G(f)$ is a quotient of this abelian group, hence is also abelian, and thus can't be S_3. This shows that f has three real roots, so that the splitting field of f is contained in $\mathbb{R}$ and hence can't be all of $\mathbb{Q}(\xi)$. It follows that the degree of the splitting field is 3, and so $G(f) \cong \mathbb{Z}/3\mathbb{Z}$.

Second proof. Since $\mathbb{Q}(\xi)/\mathbb{Q}$ is Galois with abelian Galois group, every between field is a Galois extension of $\mathbb{Q}$ (since the subgroup of the big Galois group which fixes it is a normal subgroup). Thus $\mathbb{Q}(\xi + \xi^{-1})$ is Galois, hence is itself the splitting field of $\xi + \xi^{-1}$. Since the minimal polynomial of $\xi + \xi^{-1}$ is f, a polynomial of degree 3, this extension is degree 3. The only group of order 3 is $\mathbb{Z}/3\mathbb{Z}$, hence that is what $G(f)$ must be.

3. Let L and E be finite-degree field extensions of F, which are contained in a common algebraic closure of F.

(a) Show that L/F normal $\Rightarrow$ LE/E normal.

ANSWER: Recall that an extension L/F is normal iff it is the splitting field of a polynomial in $F[X]$ (proved in class). If L/F is the splitting field of $f \in F[X]$, then clearly LE is the splitting field of f regarded as an element of $E[X]$, so LE/E is also normal.

(b) Show that L/F Galois $\Rightarrow$ LE/E Galois, and in that case $\mathrm{Gal}(LE/E)$ can be identified with a subgroup of $\mathrm{Gal}(L/F)$.

ANSWER: Recall that an extension L/F is Galois iff it is the splitting field of a *separable* polynomial $f \in F[X]$. If L/F is the splitting field of a separable polynomial $f \in F[X]$, then LE is the splitting field of f regarded as an element of $E[X]$ (and the latter is still separable, since its roots are distinct). So, LE/E is Galois.

The restriction map $\sigma \mapsto \sigma|_L$ gives a homomorphism of groups $\mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/F)$. It is injective since if $\sigma \in \mathrm{Aut}(LE)$ fixes both L and E, it fixes LE and hence is the identity element in $\mathrm{Gal}(LE/E)$.

(c) Show that if L/F and E/F are both Galois, then LE/F is Galois.

ANSWER: The proof is as in (b): Let L/F be the splitting field of a separable $f \in F[X]$, and E/F the splitting field of a separable $g \in F[X]$. Then LE is the splitting field of the square-free part of $fg \in F[X]$ (which is separable), hence LE/F is Galois.

(d) Use (c) and the notion of Galois closure to prove that if L/F and E/F are separable, then so is LE/F.

ANSWER: We proved in class that any separable extension is contained in a Galois extension (e.g. its Galois closure). Let $\widetilde{L}/F$ (resp. $\widetilde{E}/F$) be the Galois closure of the separable extension L/F (resp. E/F). Then by (c), $\widetilde{L}\widetilde{E}/F$ is Galois, hence separable. But then the subextension LE/F is also separable.

(e) For EXTRA CREDIT, similarly deduce from (c) that the set of elements in a finite-degree extension $K \supset F$ which are separable over F forms a subfield of K.

ANSWER: Let $\alpha, \beta \in K$ be separable over F. Then α (resp. β) is contained in a Galois extension L/F (resp. E/F); for example you could take the splitting field of the minimum polynomial of α (resp. β). Then by using (c) the compositum $F(\alpha, \beta) = F(\alpha)F(\beta)$ is separable over F, since it is contained in the Galois extension LE/F. But then $\alpha \pm \beta$, $\alpha\beta$ and α/β (if $\beta \neq 0$) are each separable over F elements of K.

4. Let R denote an integral domain with fraction field F. Let B be any R-module and let $t(B)$ denote the R-torsion submodule of B. Prove that $\mathrm{Tor}_1^R(F/R, B) \cong t(B)$. HINT: it might help to recall that F is a flat R-module.

ANSWER: Write $F = S^{-1}R$, where S denotes the multiplicative subset of non-zero elements in R. The short exact sequence of R-modules

$$0 \to R \to S^{-1}R \to F/R \to 0$$

gives rise upon applying the functor $- \otimes_R B$ to the long exact sequence of R-modules

$$\cdots \to \mathrm{Tor}_1^R(F, B) \to \mathrm{Tor}_1^R(F/R, B) \to B \to S^{-1}B \to F/R \otimes_R B \to 0.$$

Since F is R-flat, we have $\mathrm{Tor}_1^R(F, B) = 0$, and so $\mathrm{Tor}_1^R(F/R, B)$ is identified with the kernel of the natural map

$$B \to S^{-1}B.$$

It's clear that that kernel is just $t(B)$.

5. Let G denote a finite group and $g \in G$.

(a) Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation of G and let χ_ρ denote its character. Show that $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

ANSWER: Recall that in some basis we have $\rho(g) = \mathrm{diag}(\omega_1, \ldots, \omega_n)$, for some roots of unity ω_i, and thus we also have $\rho(g^{-1}) = \mathrm{diag}(\omega_1^{-1}, \ldots, \omega_n^{-1})$. But then

$$\overline{\chi_\rho(g)} = \sum_i \overline{\omega_i} = \sum_i \omega_i^{-1} = \chi_\rho(g^{-1}),$$

which is what we wanted to prove.

(b) Prove that g is conjugate to g^{-1} in G if and only if every irreducible character χ_ρ is real-valued on g.

ANSWER: If g is conjugate to g^{-1}, then for every representation ρ, we have $\chi_\rho(g) = \chi_\rho(g^{-1})$, since characters are class-functions. Now using (a) we see $\chi_\rho(g)$ is fixed by complex conjugation, hence is a real number.

Conversely, suppose that for every irreducible character χ_ρ we have $\chi_\rho(g) \in \mathbb{R}$, so that by (a) we have $\chi_\rho(g) = \chi_\rho(g^{-1})$. If g and g^{-1} are not conjugate, then column orthogonality gives

$$0 = \sum_\rho \chi_\rho(g)\overline{\chi_\rho(g^{-1})} = \sum_\rho \chi_\rho(g)^2.$$

Since $\chi_\rho(g) \in \mathbb{R}$, this means $\chi_\rho(g) = 0$ for each ρ. But then this violates the other assertion in column orthogonality, namely that each column in the character table has non-zero pairing with itself:

$$\sum_\rho \chi_\rho(g)\overline{\chi_\rho(g)} = |G|/|C_g|$$

where C_g is the conjugacy class of g.

Even easier: Note that $\chi_1(g) = 1$, where χ_1 denotes the trivial character.

Another proof of converse: If $\chi_\rho(g) = \chi_\rho(g^{-1})$ for all irreducible characters χ_ρ, then since these form a basis for the space of class functions on G, every class function takes the same values on g and g^{-1}. This shows that they are in the same class (otherwise, the characteristic function for the class of g would be 1 on g but 0 on g^{-1}).

(c) Show that for $G = S_n$, each element is conjugate to its inverse, and hence all characters of S_n are real-valued functions.

ANSWER: Conjugacy in S_n is given by the type of cycle decomposition. Since g and g^{-1} obviously have the same type of cycle decomposition, they are conjugate.

6. Consider the quaternion group Q_8 of order 8, with its usual presentation $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where i, j, k satisfy the relations $i^2 = j^2 = k^2 = -1$, and $ij = k$, $jk = i$, and $ki = j$.

The character table looks (in part) like:

	1	-1	i	j	k
χ_1	1	1	1	1	1
χ_2	1	1			
χ_3	1	1			
χ_4	1	1			
χ_5	2	-2			

(a) Verify that the conjugacy classes are indeed represented by the given elements, and find the orders of the conjugacy classes.

ANSWER: Clearly 1 and -1 belong to the center of Q_8, so represent conjugacy classes of size one. Note that

$$jij^{-1} = -jij = -jk = -i$$

and

$$kik^{-1} = -kik = -jk = -i.$$

These show that $\{i, -i\}$ form a conjugacy class. Similarly, the other conjugacy classes are $\{j, -j\}$ and $\{k, -k\}$.

(b) Fill in the rest of the character table, making use of the information already present in the table, and theorems we covered in class. NOTE: there is more than one correct answer, since we have not spelled out precisely which representations correspond to χ_2, χ_3 and χ_4.

ANSWER: First we determine the last row; suppose it is $(2, -2, a, b, c)$. Then

$$1 = (\chi_5, \chi_5) = \frac{1}{8}(2^2 + (-2)^2 + 2a\overline{a} + 2b\overline{b} + 2c\overline{c})$$

and the fact that $a\overline{a}$ etc are non-negative real numbers implies that $a = b = c = 0$. So the last line is $(2, -2, 0, 0, 0)$.

Now in the three remaining columns, the missing entries are all 1 or -1. To prove this, let $\chi = \chi_i$ for $i = 2, 3$ or 4. It is easy to compute the commutator group of $G = Q_8$, and it turns out to be $\{\pm 1\}$. We have $G/G' = V$, the Klein-four group, and the character χ is the composition $G \to V \to \mathbb{C}^\times$ for some character $V \to \mathbb{C}^\times$. It follows that $\chi(i) = \chi(-i)$ since $i \equiv -i \bmod G'$. But $-i = i^{-1}$, and so

$$\chi(i) = \chi(i)^{-1},$$

i.e.

$$\chi(i)^2 = 1.$$

This shows $\chi(i) = \pm 1$. This proves that all the remaining entries are ± 1.

Now to conclude, note that column orthogonality between the 2nd and 3rd columns proves that two of the missing entries in the 3rd column are -1 and the other is 1. Likewise for the 4th and 5th columns. The orthogonality between the 3rd, 4th, and 5th columns forces the negative ones to be arranged as in the final answer (which is not unique since we could permute the 3rd 4th and 5th columns around):

	1	-1	i	j	k
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0