Name: ____________________________________

Math 230C final, with solutions

June 15, 2005, 1:30-3:30pm

Closed book, no notes or other aids. Justify your answers carefully and completely. Use the back of the page if necessary, and there is a blank page at the end for extra space. There are 7 problems.

Z, **Q**, **R**, and **C** denote the integers, rational, real and complex numbers, respectively.

(12 points) 1. Suppose that $K \subset F$ are finite fields. Prove that F/K is a Galois extension and $\mathrm{Gal}(F/K)$ is cyclic.

Let $q = |K|$, so q is a power of some prime p. Let $d = [F : K]$, so $|F| = q^d$. Define $\phi : F \to F$ by $\phi(x) = x^q$. If $x, y \in F$ then $\phi(xy) = \phi(x)\phi(y)$, and since F has characteristic p, $\phi(x+y) = (x+y)^q = x^q + y^q = \phi(x) + \phi(y)$, so ϕ is an automorphism of F. Further $x^q = x$ for every $x \in K$, so ϕ restricted to K is the identity. Thus $\phi \in \mathrm{Aut}(F/K)$.

Suppose ϕ has order k in $\mathrm{Aut}(F/K)$. Then $x^{q^k} = \phi^k(x) = x$ for every $x \in F$. Since the polynomial $t^{q^k} - t$ has at most q^k roots in F, we conclude that $|F| = q^d \le q^k$ so $d \le k$. Since $|\mathrm{Aut}(F/K)| \le [F : K] = d$, we conclude that $|\mathrm{Aut}(F/K)| = d$ and ϕ is a generator. Since $|\mathrm{Aut}(F/K)| = [F : K]$, we also conclude that F/K is Galois (Lemma 4.31 and Theorem 4.34).

(12 points) 2. Classify all groups of order 275 ($= 11 \cdot 25$).

Let G be a group of order 275. The number of Sylow 11-subgroups of G is 1 modulo 11 and divides 25, so it must be 1. Therefore the Sylow 11-subgroup H is normal in G. Let K be a Sylow 5-subgroup of G; since $H \cap K = \{e\}$ and $|H||K| = |G|$ it follows that G is a semidirect product

$$G = H \rtimes_\phi K$$

for some homomorphism $\phi : K \to \mathrm{Aut}(H)$. Since H has order 11, $\mathrm{Aut}(H)$ is cyclic of order 10. Every group of order $25 = 5^2$ is abelian, so there are two possibilities for K.

Case 1: $K \cong \mathbf{Z}/25\mathbf{Z}$. In this case there are (up to composition with an automorphism of K) exactly two homomorphisms from K to $\mathrm{Aut}(H)$, the trivial one and one whose image is the (unique) subgroup of order 5. This gives rise to two groups:
G_1: the direct product $\mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$,
G_2: one nonabelian semidirect product $\mathbf{Z}/11\mathbf{Z} \rtimes \mathbf{Z}/25\mathbf{Z}$.

Case 2: $K \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$. In this case there are (up to composition with an automorphism of K) exactly two homomorphisms from K to $\mathrm{Aut}(H)$, the trivial one and one whose image is the (unique) subgroup of order 5. This gives rise to two groups:
G_3: the direct product $\mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$
G_4: one nonabelian semidirect product $\mathbf{Z}/11\mathbf{Z} \rtimes (\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z})$.

Thus every group of order 275 is isomorphic to G_i for $i = 1, 2, 3$, or 4. Further, $G_1 \ncong G_2$ since G_1 is abelian and G_2 is not, similarly $G_3 \ncong G_4$, and if $i \leq 2$ and $j \geq 3$ then $G_i \ncong G_j$ because the Sylow 5-subgroups of G_i are cyclic and the Sylow 5-subgroups of G_j are not. Thus the 4 groups G_1, G_2, G_3, G_4 are pairwise nonisomorphic.

(12 points) 3. Let R be a commutative ring with identity. An R-module F is called *flat* if whenever $f : M \to N$ is an injective homomorphism of R-modules, the induced map $M \otimes_R F \to N \otimes_R F$ is injective.

(a) Show that $\mathbf{Z}/2\mathbf{Z}$ is not a flat $\mathbf{Z}$-module.

(b) More generally, if R is a principal ideal domain and A is a nonzero finitely generated torsion R-module, show that A is not flat.

(a) Recall that if M is a $\mathbf{Z}$-module then $M \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z}) \cong M/2M$. Let $N = \mathbf{Z}$ and $M = 2\mathbf{Z}$, with the natural (injective) inclusion $M \hookrightarrow N$. Tensoring with $\mathbf{Z}/2\mathbf{Z}$ induces the *zero* map $(2\mathbf{Z}/4\mathbf{Z}) \to (\mathbf{Z}/2\mathbf{Z})$, which is not injective. (I.e., $2 \otimes 1$ in not zero in $(2\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z})$, but it is zero in $\mathbf{Z} \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z})$.) Thus $\mathbf{Z}/2\mathbf{Z}$ is not flat.

(b) By the classification theorem we have $A \cong \oplus_{i=1}^{k}(R/d_iR)$ where the d_i are nonzero non-units in R and $d_1 \mid d_2 \mid \cdots \mid d_k$. If M is an R-module then $M \otimes A \cong \oplus_i (M \otimes (R/d_iR)) \cong \oplus M/d_iM$.

As in part (a), consider the injective map $d_kR \hookrightarrow R$. Tensoring with A gives the map

$$\oplus_{i=1}^{k} d_kR/d_id_kR \to \oplus_{i=1}^{k} R/d_iR$$

which is zero since $d_kR \subset d_iR$ for every i. Thus A is not flat.

(12 points) 4. Let ρ be a representation of S_4 acting on a complex vector space, and suppose $\rho = \oplus_{i=1}^{k} \rho_i$ with irreducible representations ρ_i. Suppose that the character χ of ρ satisfies

$$\begin{aligned} \chi(e) &= 4 \quad \text{where } e \text{ is the identity} \\ \chi((1\ 2)) &= 2 \\ \chi((1\ 2\ 3)) &= 1 \\ \chi((1\ 2\ 3\ 4)) &= 0 \\ \chi((1\ 2)(3\ 4)) &= 0 \end{aligned}$$

(a) What is the dimension of ρ?
(b) What is k?
(c) How many of the ρ_i are the trivial representation?
(d) Give (explicitly) the characters of all the ρ_i.

(a) $\dim(\rho) = \chi(e) = 4$.
(b) Let $X_2, X_3, X_4, X_{2,2}$ be the sets of 2-cycles, 3-cycles, 4-cycles, and products of two disjoint 2-cycles, respectively, in S_4. Along with $\{e\}$, these are the conjugacy classes in S_4, so every character is constant on each of these sets. We also compute easily that $|X_2| = 6$, $|X_3| = 8$, $|X_4| = 6$, $|X_{2,2}| = 3$. We compute

$$\langle \chi, \chi \rangle = \frac{1}{24} \sum_{\sigma \in S_4} |\chi(\sigma)|^2 = \frac{1}{24}(4^2 + 6 \cdot 2^2 + 8 \cdot 1^2) = 2.$$

Also, if χ_i is the character of ρ_i, then

$$\langle \chi, \chi \rangle = \langle \sum_i \chi_i, \sum_j \chi_j \rangle = \sum_{i,j} \langle \chi_i, \chi_j \rangle.$$

Since $\langle \chi_i, \chi_j \rangle$ is 1 if $\chi_i = \chi_j$ and 0 otherwise, we conclude that $k = 2$ and $\chi_1 \neq \chi_2$.
(c) Let ψ be the character of the trivial representation, so $\psi(\sigma) = 1$ for every $\sigma \in S_4$. The number of ρ_i that are the trivial representation is

$$\langle \chi, \psi \rangle = \frac{1}{24} \sum_{\sigma \in S_4} \chi(\sigma)\bar{\psi}(\sigma) = \frac{1}{24}(4 + 6 \cdot 2 + 8 \cdot 1) = 1.$$

(d) We can renumber if necessary so that ρ_1 is the trivial representation, i.e., $\chi_1 = \psi$. Then $\chi = \psi + \chi_2$ so $\chi_2 = \chi - \psi$ is given by $\chi_2(e) = 3$, and $\chi_2(\sigma)$ is 1, 0, -1, or -1 if $\sigma \in X_2$, X_3, X_4, or $X_{2,2}$, respectively.

(12 points) 5. Suppose $f(x) \in \mathbf{Q}[x]$ is an irreducible polynomial of degree 5, with 3 real roots and 2 complex (non-real) roots. Let K denote the splitting field of f, and let G be the image of $\mathrm{Gal}(K/\mathbf{Q})$ in S_5, viewing $\mathrm{Gal}(K/\mathbf{Q})$ as permutations of the roots of f.

(a) Show that G contains a 2-cycle.

(b) Show that G contains a 5-cycle.

(a) Complex conjugation (restricted to K) is an element of $\mathrm{Gal}(K/\mathbf{Q})$ that switches the two complex roots and and fixes the three real roots. Hence complex conjugation gives a 2-cycle in G.

(b) Note that the map $\mathrm{Gal}(K/\mathbf{Q}) \to G$ is injective: every automorphism of K that fixes all the roots of f fixes the splitting field K of f.
Let α be a root of f in K. Since f is irreducible, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 5$. Hence $|G| = |\mathrm{Gal}(K/\mathbf{Q})| = [K : \mathbf{Q}] = 5[K : \mathbf{Q}(\alpha)]$ is divisible by 5, so G has an element of order 5. The only elements of order 5 in S_5 are 5-cycles.

(16 points) 6. For each part below, give your answer and a *brief* justification.

(a) Suppose G is a finite group, and $K \neq \{e\}$ is a subgroup of G that is contained in *every* subgroup of G other than $\{e\}$. Explain why the order of G must be a power of a prime.

(b) Give a maximal ideal of the ring $\mathbf{Z} \times \mathbf{Z}[x]$.

(c) Is $\{(n, n) : n \in \mathbf{Z}\}$ a prime ideal of $\mathbf{Z} \times \mathbf{Z}$?

(d) Give two square matrices A and B with entries in $\mathbf{Q}$, such that the minimal polynomial of A is equal to the minimal polynomial of B and the characteristic polynomial of A is equal to the characteristic polynomial of B, but A and B are *not* similar.

(a) Suppose p is a prime dividing the order of G, and let H_p be a Sylow p-subgroup of G. Then $H_p \neq \{e\}$, so $K \leq H_p$. If $|G|$ has two distinct prime factors p and q, then $K \leq H_p \cap H_q = \{e\}$, which is impossible. Thus $|G|$ is a prime power.

(b) $2\mathbf{Z} \times \mathbf{Z}[x]$ is an ideal, and it's maximal because $(\mathbf{Z} \times \mathbf{Z}[x])/(2\mathbf{Z} \times \mathbf{Z}[x]) \cong \mathbf{Z}/2\mathbf{Z}$ is a field.

(c) No. It's not an ideal because $(1, 1)$ is in it but $(1, 1)(1, 0) = (1, 0)$ is not.

(d)

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

both have characteristic polynomial x^4 and minimal polynomial x^2, but they have different elementary divisors (x^2, x, x versus x^2, x^2).

(16 points) 7. For each part below, answer True or False *and* give a *brief* justification.

(a) True or False: if F is a finite extension of $\mathbf{Q}$ in $\mathbf{C}$, and $F \not\subset \mathbf{R}$, then $[F : \mathbf{Q}]$ must be even.

(b) True or False: if F is a finite extension of $\mathbf{Q}$ in $\mathbf{C}$, and $\sqrt{-2} \in F$, then $[F : \mathbf{Q}]$ must be even.

(c) True or False: if ρ_1 and ρ_2 are irreducible complex representations of a finite group, then $\rho_1 \otimes \rho_2$ is irreducible.

(d) True or False: If A and B are finite commutative groups, and for every $n \in \mathbf{Z}^+$ we have

$$|\{a \in A : na = 0\}| = |\{b \in B : nb = 0\}|,$$

(i.e., those two sets have the same cardinality) then $A \cong B$.

(a) False: let $\alpha = e^{2\pi i/3}\sqrt[3]{2}$ where $\sqrt[3]{2}$ is the real cube root of 2. Then $\mathbf{Q}(\alpha) \not\subset \mathbf{R}$ but $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$.

(b) True: $[F : \mathbf{Q}] = [F : \mathbf{Q}(\sqrt{-2})][\mathbf{Q}(\sqrt{-2}) : \mathbf{Q}] = 2[F : \mathbf{Q}(\sqrt{-2})]$.

(c) False: for example, S_3 has an irreducible representation of degree 2 but no irreducible representations of degree 4 (and $\dim(\rho_1 \otimes \rho_2) = \dim(\rho_1)\dim(\rho_2)$).

(d) True. We can write $A = \oplus_p(\oplus_i \mathbf{Z}/p^{n_{i,p}}\mathbf{Z})$, and similarly for B. From the sequence of integers $r_{k,p} = \log_p(|\{a \in A : p^k a = 0\}|$, for $k \geq 1$, we can recover the integers $n_{i,p}$ (up to reordering) for each p, and similarly for B. (For example, $r_{k+1,p} - r_{k,p}$ is the number of $n_{i,p}$ that are larger than k.) Thus A and B will have the same elementary divisors, so they are isomorphic.