Final Exam – 12/19/07
Solutions

Instructor: T. Haines
Math 600

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

Total points: 70.

1. (a) (5 points) Let G be a finite group of order pq, where p and q are (not necessarily distinct) prime numbers. Prove that either G is abelian, or $Z(G) = 1$.

ANSWER: If $Z(G)$ has order p or q, then $G/Z(G)$ has prime order hence is cyclic. But then it follows that G is abelian, and thus $Z(G) = G$, a contradiction. So $Z(G)$ has order pq or 1.

(b) (5 points) In case $Z(G) = 1$, exhibit G as a semi-direct product of cyclic groups, and explain why this is not a direct product.

ANSWER: Let P denote a p-Sylow subgroup, and Q a q-Sylow subgroup. We must have, WLOG, $p < q$ (since if $p = q$, then G has order p^2 and then G would be abelian). But then the index of Q is the smallest prime dividing $|G|$, hence Q is normal in G. Since $Q \cap P = 1$, G is the (internal) semi-direct product $Q \rtimes P$. It can't be a direct product, because then G would be abelian.

2. Suppose $n \geq 2$.

(a) (5 points) Describe the conjugacy class of the element $(1\,2\,\cdots\,n)$ in S_n. How many elements does it have?

ANSWER: The conjugacy class consists of all n-cycles. The number of n-cycles is $n!/n = (n-1)!$.

(b) (5 points) Determine the centralizer of the element $(1\,2\,\cdots\,n)$ in S_n.

ANSWER: Let C denote the centralizer of $\pi = (1\,2\,\cdots\,n)$, and let K denote the conjugacy class of π. We know $|G|/|C| = |K|$, and so $|C| = n!/(n-1)! = n$. Now C is a group of order n, which obviously contains $\langle\pi\rangle$, which is also of order n. Hence $C = \langle\pi\rangle$.

3. (10 points) Let $K = \mathbb{F}_q$, the finite field with q elements, and let $R = K[X]$. Up to isomorphism, how many R-modules V are there which satisfy $\dim_K V = 2$? Explain your answer.

ANSWER: Clearly V is a f.g. R-module, and R is a PID. Since $\dim_K V < \infty$, it is also clear that V is a torsion module. We use the classification of torsion R-modules. We either have $V = R/(a_1) \oplus R/(a_2)$ where $a_1 | a_2$ are both monic polynomials in $\mathbb{F}_q[X]$ of degree one (hence $a_1 = a_2$), or $V = R/(a)$, where a is a monic polynomial in $\mathbb{F}_q[X]$ of degree 2. We count the polynomials in each case. For the first case, there are q possibilities. In the second case, there are q^2 possibilities. All together, we thus get $q + q^2$ modules.

4. Let R be a ring (commutative, with identity).

(a) (5 points) Suppose we have an exact sequence in the category $\underline{R - \mathrm{Mod}}$

$$0 \to M' \to M \to M'' \to 0$$

where M' and M'' are Noetherian. Show that M is Noetherian.

ANSWER: Suppose $N \subset M$ is a submodule. Denote the map $M \to M''$ by ϕ. We know that $\phi(N)$ in M'' is finitely-generated: choose a finite set of generators for this image, and then choose lifts $y_1, \ldots, y_r$ in N which map to those generators. Also, $N \cap M'$ is finitely-generated; choose generators $x_1, \ldots, x_s$ for $N \cap M'$.

We claim (and this is enough to complete the proof) that N is generated by the finite set $\{x_1, \ldots, x_s, y_1, \ldots, y_r\}$. Indeed, given $n \in N$ write $\phi(n) = a_1\phi(y_1) + \cdots + a_r\phi(y_r)$ for certain $a_i \in R$. Then note that $n - \sum_i a_i y_i \in N \cap \ker\phi = N \cap M'$, so we can write $n - \sum_{i=1}^r a_i y_i = \sum_{j=1}^s b_j x_j$, for some $b_j \in R$. This proves the claim.

(b) (5 points) Suppose we have an R-module M equipped with a filtration by R-submodules

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n = 0,$$

where M_i/M_{i+1} is a Noetherian R-module for each $i = 0, 1, \ldots, n-1$. Prove that M is a Noetherian R-module.

ANSWER: We argue by induction on n. If $n = 0$, or $n = 1$, the result is obvious. Assume $n > 1$ and that the result holds for chains of length $n - 1$. Our induction hypothesis implies that M_1 is Noetherian. Applying (a) to the exact sequence

$$0 \to M_1 \to M_0 \to M_0/M_1 \to 0$$

then shows that M_0 is also Noetherian, and we are done.

5. Let K denote a field.

(a) (5 points) Show that $K[X] \otimes_K K[Y] \cong K[X, Y]$ as K-algebras.

ANSWER: The map $f(X) \otimes g(Y) \mapsto f(X)g(Y)$ is a well-defined K-algebra homomorphism from $K[X] \otimes_K K[Y]$ to $K[X, Y]$. (I will omit the easy verification that this it is well-defined and a map of K-algebras). To see it is an isomorphism, it is enough to note that it sends the K-vector space basis element $X^i \otimes Y^j$ of $K[X] \otimes_K K[Y]$ to the K-vector space basis element $X^i Y^j$ of $K[X, Y]$ (the map is therefore an isomorphism of K-vector spaces, and in particular is one-to-one and onto).

(b) (5 points) Show that $K[X] \otimes_K K[Y]$ is a Noetherian ring. State in full any theorems you invoke.

ANSWER: By two applications of the Hilbert Basis Theorem, $K[X, Y] \cong K[X][Y]$ is Noetherian (since K is). Now use part (a) to finish.

6. (a) (5 points) Let $R = \mathbb{Z}/6\mathbb{Z}$. Show that the R-module $V = 3R$ is projective but not free.

ANSWER: From $\mathbb{Z} = 2\mathbb{Z} \oplus 3\mathbb{Z}$ it follows easily that $R = 2R \oplus 3R$. Since $3R$ is a direct summand of a free R-module (R itself), by a theorem proved in class $3R$ is a projective R-module. On the other hand, $3R$ has only 2 elements in it, and the cardinality of any free R-module is either a finite multiple of 6, or infinity. So, $3R$ is not a free R-module.

(b) (5 points) Let R be any commutative ring. Suppose that the R-modules M and N are projective. Show that $M \otimes_R N$ is projective.

ANSWER: We know that the projective modules are precisely the direct summands of free modules. Write $R^I = M \oplus M'$ and $R^J = N \oplus N'$, for some index sets I, J and some complements M', N'. By properties of tensor products we have

$$R^I \otimes_R R^J = M \otimes_R N \bigoplus M \otimes_R N' \bigoplus M' \otimes_R N \bigoplus M' \otimes_R N'.$$

Since $R^I \otimes_R R^J \cong R^{I \times J}$ is R-free, we see that $M \otimes_R N$ is a direct summand of a free R-module, hence is projective.

ANSWER ONLY ONE OF THE FOLLOWING TWO QUESTIONS. Indicate which problem you want graded, by writing “GRADE” on the appropriate page in your answer book.

7. Let p denote an odd prime.

(a) (5 points) Show that the number of p-Sylow subgroups in the symmetric group S_p is $(p-2)!$.

ANSWER: Any p-Sylow subgroup is cyclic of order p and has precisely $p-1$ generators. Moreover, if two p-Sylow subgroups share a generator, they are identical. So, the elements of order p are partitioned according to which p-Sylow subgroup they belong to. We need to count the number of elements of order exactly p. This is precisely the number of distinct p-cycles, which is $p!/p = (p-1)!$. Grouping them into distinct p-Sylow subgroups (with $p-1$ in each clump), we see that the number of p-Sylow subgroups is $(p-1)!/(p-1) = (p-2)!$.

(b) (2 points) Using the result of (a) and a Sylow theorem, give a proof of Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$.

ANSWER: By a Sylow theorem, the number n_p of p-Sylow subgroups satisfies $n_p \equiv 1\ (p)$. By part (a) we get $(p-2)! \equiv 1\ \ (p)$. Multiplying both sides by $p-1 \equiv -1\ (p)$ yields the result.

(c) (3 points) Let $P = \langle (1\,2 \cdots p) \rangle$, a p-Sylow subgroup of S_p. Let $N(P)$ denote the normalizer of P in S_p. Find the order of $N(P)$.

ANSWER: A Sylow theorem states that all p-Sylow subgroups are conjugate. It follows that $n_p = |G|/|N(P)|$. We get $|N(P)| = p!/(p-2)! = p(p-1)$.

(d) (5 points EXTRA CREDIT) Find an element in $N(P)$ which is not in P. Use this to determine the structure of $N(P)$.

ANSWER: Write $\pi = (1\,2\,\cdots\,p)$. Choose an integer g with $2 \leq g \leq p-1$ which is a primitive root modulo p (meaning: the order of g in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is $p-1$). Now π^g is still a p-cycle, so is conjugate to π; choose $\sigma \in S_p$ with $\sigma\pi\sigma^{-1} = \pi^g$. It is clear that σ normalizes $\langle\pi\rangle = P$, hence is in $N(P)$, but is not in P itself (since P is abelian and σ does not commute with π). Note that for all $i = 1, 2, \ldots$ we have $\sigma^i\pi\sigma^{-i} = \pi^{g^i}$. This shows that the order of σ is at least $p-1$. Since it can't be $p(p-1)$ (since $N(P)$ is not abelian), it must be exactly $p-1$. Now $\langle\pi, \sigma\rangle$ is a group of order $p(p-1)$, hence is all of $N(P)$. Thus, $N(P)$ is a semi-direct product of a cyclic group of order p (which is normal) and a cyclic group of order $p-1$.

8. Let p denote a prime number. Let G denote a finite group, N a *normal* subgroup of G, and P a p-Sylow subgroup of G.

(a) (5 points) Show that $N \cap P$ is a p-Sylow subgroup of N.

ANSWER: Since N is normal, NP is a group. Furthermore, a basic isomorphism theorem says $NP/N \cong P/N \cap P$. It follows that $|NP|/|N| = |P|/|N \cap P|$, and after rearranging this, that $[NP : P] = [N : N \cap P]$. Now P is a p-Sylow subgroup of NP, so p is coprime with $[NP : P]$, thus also with $[N : N \cap P]$. Now $N \cap P$ is a p-group, and the above remark says it is a p-Sylow subgroup of N.

(b) (5 points) Show that the hypothesis "N is normal" is essential in part (a). In other words, find a group G, a subgroup H and a p-Sylow subgroup $P \subset G$ such that $H \cap P$ is *not* a p-Sylow subgroup of H.

ANSWER: Let G be any group which has at least two p-Sylow subgroups P and P'. Take $H = P'$. Clearly $H \cap P$ is not H, so is not a p-Sylow subgroup of H.

There are many such groups. The smallest example is A_4: it has four 3-Sylow subgroups (see p. 111 of Dummit-Foote).