Solutions to Homework 3

Math 600, Fall 2007

11 a) (5 pts) Any group of order 33 is cyclic:
By the Sylow theorems we have $n_3 \,|\, 11$ and $n_3 \equiv 1 \pmod 3$, thus $n_3 = 1$. Similarly $n_{11} \,|\, 3$ and $n_{11} \equiv 1 \pmod{11}$, hence $n_{11} = 1$. Let $H = C_3$ and $K = C_{11}$ denote the Sylow-3 and Sylow-11 groups respectively. Note that $HK = G$ as sets. The following elementary proposition (whose proof is left as exercise) allows us to conclude that $G = C_3 \times C_{11} = C_{33}$
Proposition: Let H and K be subgroups of a group G with $H < N(K)$ and $K < N(H)$ and $H \cap K = 1$, then it follows that $hk = kh \; \forall \; h, k$ and $HK \simeq H \times K$.

11 b) (5 pts) Any group of order 35^2 is abelian:
By the same reasoning as in part a) we have unique Sylow groups H and K of order 5^2 and 7^2 respectively, satisfying the hypothesis of the proposition in part a). Thus $G = H \times K$ is abelian because H and K being groups of order p^2 are abelian. The four possibilities for G (upto isomorphism) are $C_{35} \times C_{35},\ C_5 \times C_{245},\ C_7 \times C_{175},$ and C_{1225}

12 (10 pts) Let $|G| = p^n$ and assume the result for p-groups of order $< p^n$. Suppose G is simple, then the fact that the center of a p-group is nontrivial tells us that G is abelian. It is very easy to prove that if a simple group is abelian then it is C_p (prove it). The case $G = C_p$ satisfies 'the normal series with cyclic quotients' $1 \lhd G$. So we turn our attention to the case when G has a proper normal subgroup K. By the inductive hypothesis we have two 'normal series with cyclic quotients': $1 \lhd K_1 \lhd \cdots \lhd K_m = K$ and $1 \lhd H_1 \lhd \cdots \lhd H_l = G/K$, whence we obtain a third sequence $1 \lhd K_1 \lhd \cdots \lhd K \lhd \pi^{-1}(H_1) \lhd \cdots \lhd \pi^{-1}(H_l) = G$, where $\pi : G \to G/K$ is the quotient homomorphism. The fact that this is 'a normal series with cyclic quotients' is proved by appealing to the basic isomorphism theorems applied to π.

13 a) (5 pts) Show $|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$
Consider the columns of a matrix in G as elements of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. The first column can be any nonzero vector, thus there are $p^n - 1$ choices for it, the second is independent of the first and so there are $p^n - p$ choices. The j^{th} column is independent of the first $j - 1$ columns and so it has $p^n - p^{j-1}$ choices. Thus we obtain the formula.

13 b)-e) (25 pts) Let k be any field and let $M_n(k)$ denote the set of $n \times n$ matrices with en-

tries in k. Let G be the subset of $M_n(k)$ of matrices with non-zero determinant.
We skip the (not so trivial) proof that G is a group. (For the case when $k = \mathbb{F}_p$ the proof is easy because we are able to prove $\det(A\,B) = \det(A)\det(B)$ by reducing integer matrices modulo p). Let us define four subsets of $M_n(k)$

$N = \{n \in M_n(k) \mid \ n_{ij} = 0 \text{ if } i \geq j \}$.
$D = \{d \in G \mid d_{ij} = 0 \text{ if } i \neq j\}$. Note that D is the diagonal subgroup of G
$U = 1 + N$ where 1 is the identity matrix and lastly
$B = D + N$

We claim that U and B are subgroups of G.
Consider $g \in B$ and write $g = d + n$. Note that g is a triangular matrix and it is easy to directly calculate its inverse by solving a triangular system of linear equations (this is a part of Gaussian elimination technique). Doing this we find g^{-1} is of the form $g^{-1} = d^{-1} + n'$. Thus we have shown that $U < B < G$.

Next let us prove that that $B = N_G U$.
We have $g \in N_G U \Leftrightarrow \ gNg^{-1} = N$. Let $e_{\alpha\beta},\ \alpha < \beta$ be the matrices with $\alpha\beta$ entry equal to 1 and other entries zero. The $e_{\alpha\beta}$ generate N as a k-vector space. Therefore we must show $g\, e_{\alpha\beta}\, g^{-1} \in N$. Expanding this out we get the following equation:

$$g_{i\alpha}^{-1} g_{\beta j} = 0 \ \forall \ i \geq j,\ \ \alpha < \beta \tag{1}$$

Equation (1) will imply that $g \in B$, but this takes some work. Multiply equation (1) by $g_{\alpha i}$ and sum over $i \geq j$ to get:

$$0 = g_{\beta j}(\sum_{i \geq j} g_{\alpha i} g_{i\alpha}^{-1}) = g_{\beta j}(1 - \sum_{i<j} g_{\alpha i} g_{i\alpha}^{-1}) \tag{2}$$

We set $\alpha = j$ in equation (2), to obtain

$$0 = g_{\beta j}(1 - \sum_{i<j} g_{ji} g_{ij}^{-1}) \qquad \forall\, \beta > j \tag{3}$$

Now let $j = 1$ in equation (3) to conclude that the first column of g has zero entries except for g_{11}. Now inductively assume that $g_{ts} = 0$ whenever $t > s$ and $s \leq m$. This means that the first m columns are zero below the diagonal. The base case $m = 1$ is what we just showed. Then set $j = m + 1$ in equation (3), and observe that the summation term vanishes since $g_{ji} = 0$ for $i < j = m + 1$ by the induction hypothesis. Thus $g_{\beta,m+1} = 0$ if $\beta > m + 1$, i.e. we have shown that the $m + 1^{\text{th}}$ column of g is also zero below the diagonal. Thus $g \in B$.

Returning now to the case $k = \mathbb{F}_p$, it is clear that $|U| = |N| = p^{\frac{n(n-1)}{2}}$. Thus U is a Sylow-p subgroup of G. Having shown that $B = N_G U$, we know that the number of Sylow-p groups of G is the index $[G : B]$. Moreover $|D| = (p-1)^{n-1}$ so that $|B| = (p-1)^{n-1} p^{\frac{n(n-1)}{2}}$ whence

$$[G : B] = \frac{p^n - 1}{p-1} \cdot \frac{p^{n-1} - 1}{p-1} \cdots \frac{p^2 - 1}{p-1}$$

as required.

14) (10 pts) For k dividing $|G|$ define $\psi(k) = \#\{x \in G \mid x^k = 1\}$. We are given $\psi(k) \leq k$ and are required to show that G is cyclic.

Proof 1) Let $\varphi(k) = \#\{x \in G \mid |x| = k\}$. If there is an $x \in G$ with $|x| = k$ then $\langle x \rangle$ accounts for all of $\psi(k)$ because of $\psi(k) \leq k$, and so $\varphi(k) = \phi(k)$ in this case. In case there is no such x then obviously $\varphi(k) = 0$, hence $\varphi(k) \leq \phi(k)$ in general. Summing over all divisors k of $|G|$ we see both sums are equal to $|G|$ (using $\sum_{d|n} \phi(d) = n$). But then the situation $\varphi(k) < \phi(k)$ is impossible. In particular $\varphi(|G|) > 0$ implies there is an element of order $|G|$, whence G is cyclic.

Proof 2) Let $|G| = p^e m$ with $(p, m) = 1$. Since every p-subgroup of G is contained in some Sylow p-subgroup, we have $\psi(p^e)$ equals the cardinality of the union of all Sylow-p subgroups of G. Therefore $\psi(p^e) \leq p^e$ implies that the Sylow-p group is normal for each p. By the proposition mentioned in Solution of problem 11a) we know that G is the direct product of its Sylow groups, and hence it suffices to show that the Sylow-p groups are cyclic. Let H be the Sylow-p subgroup. Suppose there is an element of order p^j in H with $p^j < p^e$ then it follows that $\psi(p^j) \geq p^j$, therefore $\psi(p^j) = p^j$ which means that H has $\phi(p^j)$ elements of order p^j. Let $\varphi(p^j)$ denote the number of elements of order p^j in H. We have shown $\varphi(p^j) - \phi(p^j) \leq 0$. Summing over $j = 0..e$ and using the fact that this sum should be zero (by the formula $\sum_{d|n} \phi(d) = n$) we obtain $\varphi(p^j) = \phi(p^j)$. In particular for $j = e$ we see that H has an element of order p^e, whence it is cyclic.