Homework I (due September 30), Math 602, Fall 2002.

BIII (a). We first prove the following proposition:

Proposition 1.1 *Given a group G, for any finite normal subgroup, H, of G and any p-Sylow subgroup P of H, we have $G = N_G(P)H$.*

Proof. For every $g \in G$, clearly, $g^{-1}Pg$ is a subgroup of $g^{-1}Hg = H$, since H is normal in G. Since $|g^{-1}Pg| = |P|$, the subgroup $g^{-1}Pg$ is also a p-Sylow subgroup of H. By Sylow II, $g^{-1}Pg$ is some conjugate of P in H, i.e.,

$$g^{-1}Pg = hPh^{-1} \quad \text{for some} \quad h \in H.$$

Thus, $ghPh^{-1}g^{-1} = P$, which implies that $gh \in N_G(P)$, so $g \in N_G(P)H$. Since the reasoning holds for every $g \in G$, we get $G = N_G(P)H$. $\square$

Now, since H is normal in G, by the second homomorphism theorem, we know that $G/H = (N_G(P)H)/H \cong N_G(P)/(N_G(P) \cap H)$. Moreover, it is clear that $N_G(P) \cap H = N_H(P)$, so $G/H \cong N_G(P)/N_H(P)$, as desired.

(b) We shall prove that every p-Sylow subgroup of $\Phi(G)$ is normal in $\Phi(G)$ (and in fact, in G). From this, we will deduce that $\Phi(G)$ has property (N). Indeed, if we inspect the proof of the proposition proved in class stating that if G is a finite group that has (N), then G is isomorphic to the product of its p-Sylow subgroups, we see that this proof only depends on the fact that every p-Sylow subgroup of G is normal in G. However, we also proved that every p-group has (N), and so, we will be able to conclude by proving that if G is a p-group and H is a q-group, then $G \prod H$ also has (N).

In order to prove that every p-Sylow subgroup of $\Phi(G)$ is normal in $\Phi(G)$, we first prove:

Proposition 1.2 *Given a finite group G, if K is any subgroup of $\Phi(G)$, then there is no proper subgroup H of G so that $G = HK$.*

Proof. Let H be a proper subgroup of G. There is some maximal subgroup M of G so that $H \leq M < G$. Since $K \leq \Phi(G)$ and $\Phi(G)$ is the intersection of all the maximal subgroups of G, we have $K \leq M$. Now, since $H \leq M$ and $K \leq M$, we have $HK \leq M < G$. Therefore, there is no proper subgroup, H, of G so that $G = HK$. $\square$

Remark: Proposition 1.2 also follows immediately from the fact (proved in class) that the elements of $\Phi(G)$ are nongenerators. If $G = HK$, with $K \subseteq \Phi(G)$ and H a proper subgroup of G, then $G = \mathrm{Gp}\{H \cup K\} = \mathrm{Gp}(H) = H$, since the elements in K are nongenerators, a contradiction (since $H < G$).

Let P be any p-Sylow subgroup of $\Phi(G)$. Since $\Phi(G)$ is normal in G, by proposition 1.1, we have

$$G = N_G(P)\Phi(G).$$

Since $P \leq \Phi(G)$, by Proposition 1.2, we must have $N_G(P) = G$, so P is normal in G, and thus, in $\Phi(G)$.

To conclude, we need the proposition

Proposition 1.3 *If G is a p-group and H is a q-group, then $G \prod H$ has (N).*

First, we prove the following simple lemma:

Lemma 1.4 *For any two group G and H,*

$$Z(G \prod H) = Z(G) \prod Z(H).$$

Proof. Given any $g \in G$ and any $h \in H$, note that for all $g' \in G$ and all $h' \in H$,

$$(g,h)(g',h') = (g',h')(g,h) \quad \text{iff} \quad gg' = g'g \quad \text{and} \quad hh' = h'h,$$

since

$$(gg', hh') = (g,h)(g',h') = (g',h')(g,h) = (g'g, h'h).$$

Therefore, $Z(G \prod H) = Z(G) \prod Z(H)$. $\square$

Proof of Proposition 1.3. The case where G and H are $\{1\}$ is trivial, so we may assume that $G \prod H$ is nontrivial. Then, either G is nontrivial or H is nontrivial. Since G is a p-group and H is a q-group, we know from class that either $Z(G)$ is nontrivial or $Z(H)$ is nontrivial. But then, $Z(G \prod H) = Z(G) \prod Z(H)$ is nontrivial, and since $Z(G \prod H)$ is normal in $G \prod H$, the factor group $(G \prod H)/Z(G \prod H) \cong (G/Z(G)) \prod (H/Z(H))$ is again the product of a p-group and a q-group, but $(G \prod H)/Z(G \prod H)$ has strictly smaller order than $G \prod H$. Thus, we can now proceed by induction on the order of $G \prod H$. The proof turns out to be identical to the proof given in class that a single p-group has (N). Indeed, this proof only uses the fact that at every step of the induction, the center of the group is nontrivial. Therefore, $G \prod H$ has (N). $\square$

By an obvious induction, any finite direct product of p_j-groups has (N), and since $\Phi(G)$ is isomorphic to the direct product of its p_j-Sylow subgroups, it has (N).

BV (a). The only interesting case is the case where G is a nontrivial finite non-simple group. So, assume that G is a nontrivial finite non-simple group and that G possesses no proper nontrivial characteristic subgroup (we have to allow the trivial subgroup because of part (b), see below). In this case, G has some nontrivial minimal normal subgroup, say H_1. For every automorphism $\varphi \in \mathrm{Aut}(G)$, the group $\varphi(H_1)$ is a normal subgroup of G.

Let H be a subgroup of G of maximal order such that $H = H_1 H_2 \cdots K_k \cong \prod_{i=1}^k H_i$, where each H_i is a normal subgroup of G isomorphic to H_1, for $i = 2, \ldots, k$. Since H_1 is normal in G, it is clear that H is normal in G. We wish to prove that H is a nontrivial characteristic subgroup of G. Since $H = H_1 H_2 \cdots H_k$ in G, for every automorphism $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(H) = \varphi(H_1)\varphi(H_2)\cdots\varphi(H_k)$. If we prove that every $\varphi(H_i)$ is a subgroup of H, then we will have proved that $\varphi(H) = H$. Assume that there is some H_i so that $\varphi(H_i)$ is not a subgroup of H. We know that $\varphi(H_i)$ is normal in G (since φ is an automorphism) and $H \cap \varphi(H_i) < \varphi(H_i)$, so that $H \cap \varphi(H_i)$ is a normal subgroup of G of order strictly smaller than than of H_1, contradicting the minimality of H_1. Therefore $H \cap \varphi(H_i) = \{1\}$, and then,

$$H\varphi(H_i) \cong H \prod \varphi(H_i).$$

Now, $H\varphi(H_i)$ is also a normal subgroup of G satisfying the same property as H, and this contradicts the fact that H is of maximal order with that property. Therefore, $\varphi(H_i) \leq H$ and H is a characteristic subgroup of G. Finally, since H is nontrivial, we must have $H = G$.

It remains to prove that H_1 is simple, since then, we will have

$$G \cong \prod_{i=1}^{k} H_i$$

where the H_i are isomorphic simple groups. Now, if H' is normal in H_1, then H' is isomorphic to the subgroup $H' \prod\{1\} \prod \cdots \prod\{1\}$ of $\prod_{i=1}^{k} H_i$, and this group is obviously normal in $\prod_{i=1}^{k} H_i$, so H' is normal in G. Therefore, since H_1 is minimal, normal in G, we deduce that $H' = \{1\}$ or $H' = H$, and H_1 is simple.

(b) Let H be minimal, normal in G (as in (a), assume that G is not simple). First, we claim:

Lemma 1.5 *For any group, G, if N is normal in G and K is a characteristic subgroup of N, then K is normal in G.*

Proof. Let φ_g denote the inner automorphism of G defined by $\varphi_g(x) = gxg^{-1}$. For every such φ_g, the restriction of φ_g to N is an automorphism, since N is normal in G, and since K is characteristic in N, we have

$$gKg^{-1} = K.$$

Since this holds for every $g \in G$, the group K is indeed normal in G. $\square$

Now, since H is normal in G, by the above fact, every characteristic subgroup of H is normal in G, which implies that either $K = \{1\}$ of $K = H$, i.e., H has no proper nontrivial characteristic subgroups. Thus, we can apply (a). If H is nonabelian, it is clear that H_1 is nonabelian, and H is isomorphic to a product of mutually isomorphic, non-abelian, simple groups. It remains to treat the case where H is abelian.

Let p be any prime dividing the order of $|H|$, and let

$$A = \{a \in H \mid a^p = 1\}.$$

Obviously, A is an elementary abelian subgroup of H. We claim that $H = A$.

First, we prove that A is a characteristic subgroup of H. Indeed, for any $\varphi \in \mathrm{Aut}(H)$ and any $a \in A$, we have

$$1 = \varphi(1) = \varphi(a^p) = \varphi(a)^p,$$

so $\varphi(a) \in A$, as desired. Furthermore, since p is a prime dividing $|H|$, we know (Cauchy) that there is some element of order p in H, and thus, $1 < A$. But then, A is a nontrivial characteristic subgroup of H, which implies that $H = A$, and H is an elementary abelian p-group.

(c) We will use the following fact:

Lemma 1.6 *If G is a solvable group, then every subgroup of G is also solvable.*

Proof. It was proved in class that a group, G, is solvable iff the strictly descending chain

$$G > \Delta^{(1)}(G) > \Delta^{(2)}(G) > \cdots > \Delta^{(t)}(G)$$

reaches $\{1\}$ after finitely many steps, where $\Delta^{(0)}(G) = G$, $\Delta^{(1)}(G) = [G, G]$ and

$$\Delta^{(j+1)}(G) = [\Delta^{(j)}(G), \Delta^{(j)}(G)] = \Delta^{(1)}(\Delta^{(j)}(G)).$$

If H is any subgroup in G, it is clear that $[H, H] \leq [G, G]$, and by induction, we get $\Delta^{(j)}(H) \leq \Delta^{(j)}(G)$ for all j. Since $\Delta^{(t)}(G) = \{1\}$, we also have $\Delta^{(t)}(H) = \{1\}$ and H is solvable. $\square$

Let H be a minimal, normal subgroup of G, and assume G solvable. Since H is normal and $[H, H]$ is characteristic in H (proved in class), by Lemma 1.5, the group $[H, H]$ is normal in G. Since H is minimal, normal in G, we deduce that either $[H, H] = H$ or $[H, H] = \{1\}$. But G being solvable, by Lemma 1.6, the group $[H, H]$ is also solvable. Therefore, $[H, H] = \{1\}$, i.e., H is abelian. Therefore, if G is solvable, any minimal, normal subgroup of G is an abelian p-group.

B VI (a). Since G is a p-group, we have $|\Phi(G)| = p^m$ and $|G/\Phi(G)| = p^d$ for some $m, n \in \mathbb{N}$. We denote by $\overline{g}$ the image in $G/\Phi(G)$ of an element $g \in G$ under the natural projection $G \longrightarrow G/\Phi(G)$. We proved in class that since G is a p-group, $G/\Phi(G)$ is an abelian elementary p-group, and the assumption $|G/\Phi(G)| = p^d$ implies that, as a vector space over $\mathbb{Z}/p\mathbb{Z}$, the vector space $G/\Phi(G)$ has dimension d. Also, by the Burnside basis theorem, any minimal system of generators for G is a collection of d elements $x_1, \ldots, x_d$ such that $\overline{x_1}, \ldots, \overline{x_d}$ is a basis of $G/\Phi(G)$.

Let $x_1, \ldots, x_d$ be such a minimal system of generators for G. Then, for all $\lambda_1, \ldots, \lambda_d \in \Phi(G)$, the elements $\lambda_1 x_1, \ldots, \lambda_d x_d$ also form a minimal system of generators for G, since $\overline{(\lambda_i x_i)} = \overline{x_i}$. Define $\mathcal{S}$ to be the set of d-tuples

$$\mathcal{S} = \{(\lambda_1 x_1, \ldots, \lambda_d x_d) \mid \lambda_i \in \Phi(G), \quad \text{with} \quad 1 \leq i \leq d\}.$$

Clearly, $|\mathcal{S}| = p^{md}$.

We have a homomorphism $\theta \colon \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G/\Phi(G)$, also denoted by bar, defined so that

$$\overline{\varphi}(g\Phi(G)) = \varphi(g)\Phi(G)$$

for all $g \in G$. If we let $K = \mathrm{Ker}\ \theta$ denote the kernel of $\theta \colon \mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G/\Phi(G)$, our plan is to show that K acts on $\mathcal{S}$, and that for every $y \in \mathcal{S}$, the stabilizer, $\mathrm{Stab}_K(y)$, of y is trivial. Then, for every subgroup H of K, we will also have an action of H on $\mathcal{S}$ with the same property, namely the stabilizer, $\mathrm{Stab}_K(y)$, of any $y \in \mathcal{S}$ is trivial. Then, since $\mathcal{S}$ is the union of disjoint orbits, we will conclude that $|H|$ divide $|\mathcal{S}|$, and from this, we will get (a).

Now, observe that if $\overline{\varphi} = \mathrm{id}$, i.e., $\overline{\varphi} \in K = \mathrm{Ker}\ \theta$, then

$$\overline{\varphi(\lambda_i x_i)} = \overline{\varphi(\lambda)\varphi(x_i)} = \varphi(x_i)\Phi(G) = \overline{\varphi}(x_i\Phi(G)) = x_i\Phi(G) = \overline{x_i},$$

since $\overline{\varphi} = \mathrm{id}$. This shows that for every $\varphi \in K$ and every $(y_1, \ldots y_d) \in \mathcal{S}$, we have $(\varphi(y_1), \ldots \varphi(y_d)) \in \mathcal{S}$. Therefore, we can define an action of K on $\mathcal{S}$ by

$$\varphi \cdot (y_1, \ldots, y_d) = (\varphi(y_1), \ldots, \varphi(y_d)),$$

for every $\varphi \in K$ and every $(y_1, \ldots, y_d) \in \mathcal{S}$. Consider the stabilizer $\mathrm{Stab}_K(y)$ of any element $y = (y_1, \ldots, y_d) \in \mathcal{S}$. This group consists of those $\varphi \in K$ so that

$$(\varphi(y_1), \ldots, \varphi(y_d)) = (y_1, \ldots, y_d),$$

that is, $\varphi(y_i) = y_i$ for $i = 1, \ldots, d$. However, we observed earlier that any $(y_1, \ldots, y_d) \in \mathcal{S}$ is a minimal system of generators of G, and thus, $\varphi = \mathrm{id}$. Therefore, $\mathrm{Stab}_K(y) = \{\mathrm{id}\}$ for every $y \in \mathcal{S}$ and every orbit has size $|K|$.

Now, let H be the cyclic group generated by the automorphism $\varphi \in \mathrm{Aut}(G)$. Since we are assuming that φ has order n, the group H has order n. If $\overline{\varphi} = \mathrm{id}$, then it is obvious that $\overline{\varphi^i} = \mathrm{id}$ for all i, and so, $H \leq K$. The restriction to H of the action of K on $\mathcal{S}$ is an action of H on $\mathcal{S}$, and of course $\mathrm{Stab}_H(y) = \{\mathrm{id}\}$ for every $y \in \mathcal{S}$, so every orbit consists of $|H|$ elements. Since $\mathcal{S}$ is the union of disjoint orbits, $|H|$ divides $|\mathcal{S}|$. However, $|H| = n$, $|\mathcal{S}| = p^{md}$, and since we are assuming that $(n, p) = 1$, we must have $n = 1$. This proves that $\varphi = \mathrm{id}$, as desired.

(b) Since every linear map is determined by its action on a basis, it is clear that $|\mathrm{GL}(G/\Phi(G))|$ is just the number of ordered bases of d elements over $\mathbb{Z}/p\mathbb{Z}$. Now, $|G/\Phi(G)| = p^d$, and we can pick $p^d - 1$ nonzero vectors, u_1, as the first basis vector, $p^d - p$ vectors, u_2, other than a scalar multiple of u_1, as the second basis vector, $p^d - p^2$ vectors, u_3, other than a linear combination of u_1 and u_2, as the third basis vector, etc. Therefore,

$$\begin{aligned} |\mathrm{GL}(G/\Phi(G))| &= (p^d - 1)(p^d - p) \cdots (p^d - p^{d-1}) \\ &= (p^d - 1)p(p^{d-1} - 1) \cdots p^{d-1}(p - 1) \\ &= p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d} (p^k - 1). \end{aligned}$$

If P is any p-Sylow subgroup of $\mathrm{GL}(G/\Phi(G))$, since $|P|$ is the largest p-power dividing $|\mathrm{GL}(G/\Phi(G))|$, we must have $|P| = p^{\frac{d(d-1)}{2}}$, since p is relatively prime to $\prod_{k=1}^{d}(p^k - 1)$. This implies that

$$\sigma^{p^{\frac{d(d-1)}{2}}} = \mathrm{id},$$

and since $\det(\sigma^k) = \det(\sigma)^k$ for all $k \in \mathbb{N}$, we have

$$\det(\sigma)^{p^{\frac{d(d-1)}{2}}} = 1.$$

However, $a^p = a$ for all $a \in \mathbb{Z}/p\mathbb{Z}$ (since p is prime), so

$$\det(\sigma) = \det(\sigma)^{p^{\frac{d(d-1)}{2}}} = 1,$$

which shows that $\sigma \in \mathrm{SL}(G/\Phi(G))$.

(c) Given any p-Sylow subgroup, P, of $\mathrm{GL}(G/\Phi(G))$, let

$$\mathcal{P} = \{\varphi \in \mathrm{Aut}(G) \mid \overline{\varphi} \in P\}.$$

For every $\varphi \in \mathrm{Aut}(G)$, we may assume that the order, n, of φ is of the form $n = p^a t$ for some $a, t \in \mathbb{N}$, where t is relatively prime to p.

We claim that if $\varphi \in \mathcal{P}$, then

$$\overline{\varphi^{p^a}} = \mathrm{id}.$$

If so, since φ^{p^a} has order t relatively prime to p, by part (a), we deduce that

$$\varphi^{p^a} = \mathrm{id},$$

and thus, $t = 1$. Since this is true for every $\varphi \in \mathcal{P}$, we conclude that $\mathcal{P}$ is a p-subgroup of $\mathrm{Aut}(G)$.

It remains to prove that if $\varphi \in \mathcal{P}$, then

$$\overline{\varphi^{p^a}} = \mathrm{id}.$$

For any $\psi \in \mathrm{Aut}(G)$, if $\psi^n = \mathrm{id}$ then $(\overline{\psi})^n = \mathrm{id}$, and we see that the order of $\overline{\psi}$ divides the order of ψ. Since P is a p-Sylow subgroup of $\mathrm{GL}(G/\Phi(G))$, the order of $\overline{\varphi}$ is some p-power, p^b, and we must have $p^b \leq p^a$, since p^b divides $p^a t$ and t is relatively prime to p. So,

$$\overline{\varphi^{p^a}} = \mathrm{id},$$

as claimed.

Remark: We can prove that $|\mathrm{Aut}(G)|$ divides $p^{md} p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d}(p^k - 1)$. Going back to (a), where we defined an action of $K = \mathrm{Ker}\ \theta$ on $\mathcal{S}$, recall that we proved that every orbit has size $|K|$. Since $\mathcal{S}$ is a disjoint union of orbits, $|K|$ must divide $|\mathcal{S}| = p^{md}$. We know that $|\mathrm{Aut}(G)| = |\mathrm{Ker}\ \theta||\mathrm{Im}\ \theta|$, and since $\mathrm{Im}\ \theta$ is a subgroup of $|\mathrm{GL}(G/\Phi(G))|$, we see that $|\mathrm{Im}\ \theta|$ divides $|\mathrm{GL}(G/\Phi(G))| = p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d}(p^k - 1)$. Thus, $|\mathrm{Aut}(G)|$ divides $p^{md} p^{\frac{d(d-1)}{2}} \prod_{k=1}^{d}(p^k - 1)$.