Homework 1

Solutions

Problem 1. Let G be a group with a normal subgroup N and a (not necessarily normal) subgroup H. Suppose that N has a chain of normal (in N) subgroups

$$N_1 = N \geq N_2 \geq N_3 \geq ...$$

such that $[H, N_i] \subseteq N_{i+1}$ for all i. Prove that $[\gamma_i(H), N_j] \subseteq N_{i+j}$ for all i, j.

Solution: Note that the only elements involved in the problem are those in the subgroup NH. Replacing G by NH if necessary, we may assume that $G = NH$. Note that the inclusion $[H, N_i] \subseteq N_{i+1} \subseteq N_i$ implies that H normalizes each N_i. Since N_i is normal in N, both H and N normalize N_i, so N_i is normal in $NH = G$.

The proof that $[\gamma_i(H), N_j] \subseteq N_{i+j}$ is by induction on i and it is exactly the same as the proof given in class for the special case when $H = N = G$ and $N_j = \gamma_j(G)$. Since $H = \gamma_1(H)$, the result holds for $i = 1$ and all j.

Recall that the main tool was the following result: if A, B, C are subgroups of a group G and K is a normal subgroup of G such that both $[C, A, B]$ and $[B, C, A]$ are contained in K then $[A, B, C] \subseteq K$. Recall also that $[A, B] = [B, A]$ for any subsets A, B.

Our goal is to show that $[\gamma_{i+1}(H), N_j] \subseteq N_{i+j+1}$. Note that $\gamma_{i+1}(H) = [\gamma_i(H), H]$ so $[\gamma_{i+1}(H), N_j] = [\gamma_i(H), H, N_j]$. Applying our main tool with $A = \gamma_i(H)$, $B = H$, $C = N_j$ and $K = N_{i+j+1}$ we see that it suffices to show that $[N_j, \gamma_i(H), H] \subseteq N_{i+j+1}$ and $[H, N_j, \gamma_i(H)] \subseteq N_{i+j+1}$. Observe that

$$[N_j, \gamma_i(H), H] = [[N_j, \gamma_i(H)], H] = [H, [\gamma_i(H), N_j]] \subseteq [H, N_{i+j}] \subseteq N_{i+j+1},$$

where we used the inductive assumption that $[\gamma_i(H), N_j] \subseteq N_{i+j}$. Similarly,

$$[H, N_j, \gamma_i(H)] = [[H, N_j], \gamma_i(H)] = [\gamma_i(H), [H, N_j]] \subseteq [\gamma_i(H), N_{j+1}] \subseteq N_{i+j+1},$$

where we used the inductive assumption that $[\gamma_i(H), N_{j+1}] \subseteq N_{i+j+1}$. This completes the proof.

Problem 2. Let P be a finite p-group.

a) Prove that if $\gamma_2(P) \cap \mathfrak{z}_2(P)$ is cyclic then $\gamma_2(P)$ is cyclic.

Solution: Suppose that $\gamma_2(P)$ is not cyclic. Then, by a result from class, the group $\gamma_2(P)$ has an elementary abelian subgroup A of order p^2 which is normal in P (note that $\gamma_2(P)$ is contained in $\mathrm{Frat}(P)$). Another result from class states that a normal subgroup of order p^k is contained in $\mathfrak{z}_k(P)$. Thus $A \subseteq \gamma_2(P) \cap \mathfrak{z}_2(P)$, which contradicts the assumption that $\gamma_2(P) \cap \mathfrak{z}_2(P)$ is cyclic.

b) If the center of $[P, P]$ is cyclic then $[P, P]$ is cyclic.

Solution: Since $[P, P] = \gamma_2(P)$ commutes with $\mathfrak{z}_2(P)$, the group $\gamma_2(P) \cap \mathfrak{z}_2(P)$ is contained in the center of $[P, P]$, hence it is cyclic. By part a) the group $[P, P]$ is cyclic as well.

c) If the center of $\mathrm{Frat}(P)$ is cyclic then $\mathrm{Frat}(P)$ is cyclic.

Solution: Suppose that $\mathrm{Frat}(P)$ is not cyclic. Then, by a result from class, $\mathrm{Frat}(P)$ has an elementary abelian subgroup B of order p^2 which is normal in P. The group P acts by conjugation on B so $P/C_P(B)$ embeds into the group of automorphisms of B, which has

order $(p^2-1)(p^2-p) = p(p-1)(p^2-1)$. It follows that the group $P/C_P(B)$ has order at most p. Thus either $C_P(B) = P$ or $C_P(B)$ is a maximal subgroup of P. In both cases $\mathrm{Frat}(P) \subseteq C_P(B)$. But this implies that B is in the center of $\mathrm{Frat}(P)$, which is cyclic, a contradiction.

Problem 3. Let P be a finite p-group such that $[P^{(1)} : P^{(2)}] \leq p^2$. Prove that the commutator subgroup $P^{(1)}$ of P is abelian.

Solution: Suppose that $P^{(1)} = [P, P]$ is not abelian, i.e. that $P^{(2)}$ is not trivial. Then $P^{(2)}$ has a subgroup M of index p which is normal in P. Let $Q = P/M$. Then $Q^{(1)} = P^{(1)}/M$ and $Q^2 = P^{(2)}/M$. Thus $|Q^{(2)}| = p$ and $[Q^{(1)} : Q^{(2)}] = [P^{(1)} : P^{(2)}] \leq p^2$. In particular, $|Q^{(1)}| \leq p^3$. Since $Q^{(2)}$ is not trivial, the group $Q^{(1)}$ is not abelian and therefore we must have $|Q^{(1)}| = p^3$. There is a normal subgroup B of Q of order p^2 such that $B \subseteq Q^{(1)} = \gamma_2(Q)$. It follows that $B \subseteq \mathfrak{z}_2(Q)$. Since $\gamma_2(Q)$ and $\mathfrak{z}_2(Q)$ commute, B is a central subgroup of $Q^{(1)}$. Since $Q^{(1)}/B$ is cyclic (has order p), the group $Q^{(1)}$ is abelian, a contradiction.

Problem 4. The lower p-central series of G is the descending central series

$$G = \lambda_1(G) \geq \lambda_2(G) \geq \lambda_3(G) \geq ...$$

of subgroups of G, where $\lambda_{i+1}(G) = [\lambda_i(G), G]\lambda_i(G)^p$ for all i. Prove that

a) If $G = G_1 \geq G_2 \geq G_3 \geq ...$ is a descending central series such that G_i/G_{i+1} has exponent p for all i, then $\lambda_i(G) \subseteq G_i$ for all i.

Solution: The proof is by induction on i. For $i = 1$ the result holds trivially. Suppose that $\lambda_i(G) \subseteq G_i$ for some i. Since the G_j's form a central (descending) series, we have $[\lambda_i(G), G] \subseteq [G_i, G] \subseteq G_{i+1}$. Furthermore, $\lambda_i(G)^p \subseteq G_i^p \subseteq G_{i+1}$, the last inclusion being a consequence of the assumption that G_i/G_{i+1} has exponent p. Thus $\lambda_{i+1}(G) = [\lambda_i(G), G]\lambda_i(G)^p \subseteq G_{i+1}$.

b) $[\lambda_i(G), \lambda_j(G)] \leq \lambda_{i+j}(G)$ for all i, j.

Solution: We prove that $[\lambda_i(G), \lambda_j(G)] \leq \lambda_{i+j}(G)$ by induction on i. The proof is similar to the solution of Problem 1, but slightly more complicated. For $i = 1$ the result holds for all j since $[G, \lambda_j(G)] \leq \lambda_{1+j}(G)$ from the definition of the lower p-central series. Suppose that $[\lambda_i(G), \lambda_j(G)] \leq \lambda_{i+j}(G)$ for some i and all j.

We need the following simple result: if A, B, C are normal subgroups of a group G then $[AB, C] = [A, C][B, C]$. It is an immediate consequence of the identity $[ab, c] = [a, c]^b[b, c] = [a^b, c^b][b, c]$. Since the groups $\lambda_i(G)$, $[\lambda_i(G), G]$ and $\lambda_i(G)^p$ are all normal (even characteristic) in G, we see that

$$[\lambda_{i+1}(G), \lambda_j(G)] = [[\lambda_i(G), G]\lambda_i(G)^p, \lambda_j(G)] = [[\lambda_i(G), G], \lambda_j(G)][\lambda_i(G)^p, \lambda_j(G)].$$

Thus we need to show that $[[\lambda_i(G), G], \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$ and $[\lambda_i(G)^p, \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$.

In order to show that $[[\lambda_i(G), G], \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$ we use the same technique we employed in the solution to Problem 1. It suffices to show that both $[\lambda_j(G), \lambda_i(G), G]$ and $[G, \lambda_j(G), \lambda_i(G)]$ are contained in $\lambda_{i+j+1}(G)$. We have

$$[\lambda_j(G), \lambda_i(G), G] = [[\lambda_j(G), \lambda_i(G)], G] = [[\lambda_i(G), \lambda_j(G)], G] \subseteq [\lambda_{i+j}(G), G] \subseteq \lambda_{i+j+1}(G)$$

and

$$[G, \lambda_j(G), \lambda_i(G)] = [[\lambda_j(G), G], \lambda_i(G)] \subseteq [\lambda_{j+1}(G), \lambda_i(G)] = [\lambda_i(G), \lambda_{j+1}(G)] \subseteq \lambda_{i+j+1}(G),$$

which proves that indeed $[[\lambda_i(G), G], \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$.

It remains to prove that $[\lambda_i(G)^p, \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$. Recall that H^k denotes the subgroup of H generated by all k-th powers of elements in H. Thus every element of $\lambda_i(G)^p$ is of the form $a_1^p a_2^p ... a_k^p$ for some $a_1, ..., a_k \in \lambda_i(G)$. Observe that if $x, y \in \lambda_i(G)$ and $z \in \lambda_j(G)$ then $[x, z], [y, z]$ are in $\lambda_{i+j}(G)$ by the inductive assumption. Since $[G, \lambda_j(G)] \leq \lambda_{1+j}(G)$, we see that the elements of $\lambda_{i+j}(G)$ are central modulo $\lambda_{1+i+j}(G)$. Thus for $a, b \in \lambda_i(G)$ and any $c \in \lambda_j(G)$ we have

$$[ab, c] = [a, c]^b [b, c] \equiv [a, c][b, c] \bmod \lambda_{i+j+1}(G).$$

It follows that for $a = a_1^p a_2^p ... a_k^p \in \lambda_i(G)^p$ and any $c \in \lambda_j(G)$ we have

$$[a, c] = [a_1^p a_2^p ... a_k^p . c] \equiv [a_1, c]^p [a_2, c]^p ... [a_k, c]^p \bmod \lambda_{i+j+1}(G).$$

Since $[a_s, c] \in \lambda_{i+j}(G)$ for $s = 1, ..., k$ we see that $[a_s, c]^p \in \lambda_{1+i+j}(G)$ for all s. Thus $[a_1, c]^p [a_2, c]^p ... [a_k, c]^p \in \lambda_{1+i+j}(G)$ and therefore $[a, c] \in \lambda_{1+i+j}(G)$. This proves that $[\lambda_i(G)^p, \lambda_j(G)] \subseteq \lambda_{i+j+1}(G)$ and completes our proof of b).

c) If $\lambda_2(G) = \gamma_2(G)$ then $\lambda_i(G) = \gamma_i(G)$ for all i.

Solution: Note that $\gamma_i(G) \subseteq \lambda_i(G)$ for all i, since $G = \lambda_1(G) \geq \lambda_2(G) \geq \lambda_3(G) \geq ...$ is a central series. By part a), in order to show that $\lambda_i(G) \subseteq \gamma_i(G)$ it suffices to prove that $\gamma_i(G)/\gamma_{i+1}(G)$ has exponent p. The group $\gamma_i(G)/\gamma_{i+1}(G)$ is abelian, so it would be enough to show that it is generated by elements of order p. For $i = 1$ this follows from the assumption that $\lambda_2(G) = \gamma_2(G)$. Suppose that $i \geq 2$. The group $\gamma_i(G)/\gamma_{i+1}(G)$ is generated by elements of the form $[g, u]\gamma_{i+1}(G)$ with $g \in G$ and $u \in \gamma_{i-1}(G)$. Note that for $g, h \in G$ and $u \in \gamma_{i-1}(G)$ we have $[gh, u] = [g, u]^h [h, u] = [g, u][[g, u], h][h, u]$. Since $[[g, u], h] \in \gamma_{i+1}(G)$, we conclude that $[gh, u]\gamma_{i+1}(G) = [g, u]\gamma_{i+1}(G)[h, u]\gamma_{i+1}(G)$. Consequently, $([g, u]\gamma_{i+1}(G))^p = [g^p, u]\gamma_{i+1}(G)$. It follows from the equality $\lambda_2(G) = \gamma_2(G)$ that $g^p \in \gamma_2(G)$ for all $g \in G$. Thus $[g^p, u] \in \gamma_{i+1}(G)$ for all $g \in G$ and $u \in \gamma_{i-1}(G)$. Hence $([g, u]\gamma_{i+1}(G))^p = 1$ for all $g \in G$ and $u \in \gamma_{i-1}(G)$, which proves that the group $\gamma_i(G)/\gamma_{i+1}(G)$ is generated by elements of order p.

Problem 5. Prove that if a finite p-group has an abelian subgroup of index p^2 then it has a normal abelian subgroup of index p^2.

Solution: Let A be an abelian subgroup of index p^2 in P. Suppose that A is not normal and let M be a maximal subgroup of P which contains A. Thus M is normal in P and A is maximal in M. Since A is not normal, there is $g \in P$ such that $gAg^{-1} \neq A$. Note that $gAg^{-1} \subseteq gMg^{-1} = M$. Thus A and gAg^{-1} are distinct maximal subgroups of M so $A(gAg^{-1}) = M$. Since A and gAg^{-1} are abelian, the group $K = A \cap gAg^{-1}$ is central in $A(gAg^{-1}) = M$. Clearly K has index p^2 in M so the center $Z(M)$ of M has index at most p^2. If the index $[M : Z(M)] \leq p$ then M is abelian and there is as a subgroup B of index p in M which is normal in P, so B is an abelian normal subgroup of P of index p^2. If the index $[M : Z(M)] = p^2$ then since both M and $Z(M)$ are normal in P, there is a subgroup $Z(M) < C < M$ normal in P. Clearly C has index p^2 in P and is abelian (since $C/Z(M)$ is cyclic). Thus in any case, P has a normal abelian subgroup of index p^2.

Problem 6. Let p be a prime and let $\mathbb{F}_p$ be the field with p-elements. Find the lower central series and the derived series of the group of $n \times n$ upper-triangular matrices over $\mathbb{F}_p$ with all diagonal entries equal to 1.

Solution: Denote the group of $n \times n$ upper-triangular matrices over a field F with all diagonal entries equal to 1 by $\mathrm{UT}(n,F)$ (elements of this group are called **unipotent upper-triangular matrices**). Let $\mathrm{UT}_k(n,F)$ be the subset of $\mathrm{UT}(n,F)$ which consists of all unipotent upper-triangular matrices whose first $k-1$ diagonals above the main diagonal are zero. In other words, a unipotent upper-triangular matrix $(a_{i,j})$ belongs to $\mathrm{UT}_k(n,F)$ iff $a_{i,j}=0$ for all i,j such that $0<j-i<k$. Clearly $\mathrm{UT}_1(n,F)=\mathrm{UT}(n,F)$ and it is a simple exercise to show that $\mathrm{UT}_k(n,F)$ is a normal subgroup of $\mathrm{UT}(n,F)$ for all k. The simplest way to do that is to think of elements of $\mathrm{UT}(n,F)$ as linear transformations.

Recall that $n \times n$ matrices can be naturally identified with linear transformations on the vector space $V=F^n$. Denote by V_i the subspace of V which consists of vectors with all but the first i coordinates equal to 0. Thus $V_0=\{0\}$, $V_1=\{(a,0,0,...,0): a\in F\}$, etc. Via the identification of matrices and linear transformation we have

$$\mathrm{UT}_k(n,F)=\{T: V \longrightarrow V : (T-I)(V_i)\subseteq V_{i-k} \text{ for all } k\}$$

(where we set $V_i=\{0\}$ for $i<0$). In particular, $T(V_i)=V_i$ for all $T\in \mathrm{UT}(n,F)$. If $S\in \mathrm{UT}_k(n,F)$ then $(TST^{-1}-I)(V_i)=T(S-I)T^{-1}(V_i)=T(S-I)(V_i)\subseteq T(V_{i-k})=V_{i-k}$ for any $T\in \mathrm{UT}(n,F)$, proving that $\mathrm{UT}_k(n,F)$ is a normal subgroup of $\mathrm{UT}(n,F)$.

For any $i\neq j$ let $e_{i,j}$ denote the matrix with i,j-entry 1 and all other entries 0. For $a\in F$ set $E_{i,j}(a)=I+ae_{i,j}$. This is the familiar elementary matrix: the product $E_{i,j}(a)M$ is obtained from M by adding to the i-th row of M the j-th row multiplied by a.

Note that $E_{i,j}(a)\in \mathrm{UT}_k(n,F)$ iff $j-i\geq k$. The key observation is the following

Lemma 1. *The group $UT_k(n,F)$ is generated by the set $\{E_{i,j}(a): j-i\geq k \text{ and } a\in F\}$.*

Proof: The proof is a simple consequence of the familiar row reduction process. Let $A=(a_{i,j})\in \mathrm{UT}_k(n,F)$. The matrix

$$B=E_{n-k,n}(-a_{n-k,n})...E_{2,k+2}(-a_{2,k+2})E_{1,k+1}(-a_{1,k+1})A$$

has 0's in the $k-th$ diagonal over the main diagonal, i.e all the entries of the form $i,i+k$ are zero. But this matrix belongs to $\mathrm{UT}_k(n,F)$, since all the elementary matrices used are in this group. Thus $B\in \mathrm{UT}_{k+1}(n,F)$. Note that

$$A=E_{1,k+1}(a_{1,k+1})E_{2,k+2}(a_{2,k+2})...E_{n-k,n}(a_{n-k,n})B,$$

This shows that if Lemma 1 holds for $\mathrm{UT}_{k+1}(n,F)$ then it also holds for $\mathrm{UT}_k(n,F)$. Since $\mathrm{UT}_{n-1}(n,F)=\{E_{1,n}(a): a\in F\}$, Lemma 1 holds for $\mathrm{UT}_{n-1}(n,F)$ and therefore it holds for all k by (now) obvious induction. □

Lemma 2. $[\mathrm{UT}_i(n,F),\mathrm{UT}_j(n,F)]\subseteq \mathrm{UT}_{i+j}(n,F)$

Proof: We will use the approach via liner transformations. Let $T\in \mathrm{UT}_i(n,F)$ and $S\in \mathrm{UT}_j(n,F)$. Then

$$[T,S]-I=T^{-1}S^{-1}TS-I=T^{-1}S^{-1}(TS-ST)=T^{-1}S^{-1}((T-I)(S-I)-(S-I)(T-I)).$$

Now $(T-I)(S-I)(V_k)\subseteq (T-I)(V_{k-j})\subseteq V_{k-i-j}$ and likewise $(S-I)(T-I)(V_k)\subseteq V_{k-i-j}$. It follows that $((T-I)(S-I)-(S-I)(T-I))(V_k)\subseteq V_{k-i-j}$ and therefore

$$([T,S]-I)(V_k)=T^{-1}S^{-1}((T-I)(S-I)-(S-I)(T-I))(V_k)\subseteq T^{-1}S^{-1}(V_{k-i-j})\subseteq V_{k-i-j}.$$

This shows that $[T,S]\in \mathrm{UT}_{i+j}(n,F)$. □

We will prove now that in Lemma 2 equality holds. By Lemma 1, it suffices to show that $E_{s,t}(a) \in [\mathrm{UT}_i(n,F), \mathrm{UT}_j(n,F)]$ for all $a \in F$ and all s,t such that $t-s \geq i+j$. Recall the following simple but very useful identities:

$$[E_{k,l}(a), E_{p,q}(b)] = \begin{cases} 1 & \text{if } k \neq q \text{ and } l \neq p; \\ E_{k,q}(ab) & \text{if } l = p \text{ and } k \neq q; \\ E_{p,l}(-ab) & \text{if } k = q \text{ and } l \neq p \end{cases}$$

In particular, if $t-s \geq i+j$ then $t-(s+i) \geq j$ so $E_{s,t}(a) = [E_{s,s+i}(1), E_{s+i,t}(a)]$ and $E_{s,s+i}(1) \in \mathrm{UT}_i(n,F)$, $E_{s+i,t}(a) \in \mathrm{UT}_j(n,F)$. Thus we proved

Lemma 3. $[\mathrm{UT}_i(n,F), \mathrm{UT}_j(n,F)] = \mathrm{UT}_{i+j}(n,F)$

It is now not hard to derive the following

Theorem 1. $\gamma_i(\mathrm{UT}(n,F)) = \mathrm{UT}_i(n,F)$ *and* $\mathrm{UT}(n,F)^{(k)} = \mathrm{UT}_{2^k}(n,F)$. *The nilpotency class of* $\mathrm{UT}(n,F)$ *is* $n-1$ *and the derived length is* $\lceil \log_2 n \rceil$.

Proof: Lemma 3 and simple induction prove the theorem. In fact, for $i=1$ and $k=0$ the theorem is trivially true. If it holds for some i and k then

$$\gamma_{i+1}(\mathrm{UT}(n,F)) = [\gamma_i(\mathrm{UT}(n,F)), \gamma_1(\mathrm{UT}(n,F))] = [\mathrm{UT}_i(n,F), \mathrm{UT}_1(n,F)] = \mathrm{UT}_{i+1}(n,F)$$

and

$$\mathrm{UT}(n,F)^{(k+1)} = [\mathrm{UT}(n,F)^{(k)}, \mathrm{UT}(n,F)^{(k)}] = [\mathrm{UT}_{2^k}(n,F), \mathrm{UT}_{2^k}(n,F)] =$$
$$= \mathrm{UT}_{2^k+2^k}(n,F) = \mathrm{UT}_{2^{k+1}}(n,F).$$

Since $\mathrm{UT}_i(n,F) = 1$ iff $i \geq n$, the last claim of the theorem follows. $\square$

Remark. Note that our solution works over an arbitrary field. The group $\mathrm{UT}(n,F)$ is a finite $p-$group iff F is a finite field of characteristic p.