Homework 2
Solutions

Problem 1. Let F be a field.

a) Let $\phi : \mathrm{UT}(n,F) \longrightarrow \mathrm{UT}(n-1,F)$ be a function such that $\phi(A)$ is the matrix obtained from A after removing its last row and its last column. Prove that ϕ is a surjective group homomorphism.

b) Let $\psi : \mathrm{UT}(n,F) \longrightarrow \mathrm{UT}(n-1,F)$ be a function such that $\psi(A)$ is the matrix obtained from A after removing its first row and its first column. Prove that ψ is a surjective group homomorphism.

Solution: Both a) and b) follow easily from the definition of matrix multiplication. A more conceptual argument is based on interpretation of $\mathrm{UT}(n,F)$ as linear transformations. 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

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

The map $\phi : \mathrm{UT}(n,F) \longrightarrow \mathrm{UT}(n-1,F)$ is just the restriction map which sends $T \in \mathrm{UT}_k(n,F)$ to its restriction to the space V_{n-1}. Similarly, ψ sends T to the transformation induced by T on the quotient space V/V_1.

c) Prove that $\mathfrak{z}_i(\mathrm{UT}(n,F)) = \mathrm{UT}_{n-i}(n,F) = \gamma_{n-i}(\mathrm{UT}(n,F))$.

Solution. In Problem 6 of the first assignment we proved that $\mathrm{UT}_i(n,F) = \gamma_i(\mathrm{UT}(n,F))$. It follows that the group $\mathrm{UT}(n,F)$ is nilpotent of class $n-1$. We have seen in class that $\gamma_{n-i}(G) \subseteq \mathfrak{z}_i(G)$ for any nilpotent group of class $n-1$. It remains to prove that $\mathfrak{z}_i(\mathrm{UT}(n,F)) \subseteq \mathrm{UT}_{n-i}(n,F)$.

The first step is to note that the center $\mathfrak{z}_1(\mathrm{UT}(n,F)) \subseteq \mathrm{UT}_{n-1}(n,F)$. Suppose then that $A = (a_{i,j})$ is in the center. In particular, A commutes withe all the elementary matrices $E_{i,j}(1)$, $i < j$. Suppose that $i > 1$. For any $j > i$ the $1,j$ entry of $E_{1,i}(1)A$ equals $a_{1,j} + a_{i,j}$. On the other hand, the matrix $AE_{1,i}(1)$ differs from A only at entries in the i-th column so the $1,j$ entry of $AE_{1,i}(1)$ is $a_{1,j}$. It follows that $a_{1,j} + a_{i,j} = a_{1,j}$, i.e. $a_{i,j} = 0$. We see that the non-zero entries of A must be in the first row. Similarly, if $j < n$ then for any $i < j$ the i,n entry of $AE_{j,n}(1)$ is $a_{i,n} + a_{i,j}$ and the i,n entry of $E_{j,n}(1)A$ is equal to $a_{i,n}$. Thus $a_{i,j} = 0$, which shows that the non-zero entries of A must be in the last column. Combining these observations we conclude that the only entry of A which can be non-zero is the $1,n$ entry, i.e. $A \in \mathrm{UT}_{n-1}(n,F)$.

Now we prove that $\mathfrak{z}_i(\mathrm{UT}(n,F)) \subseteq \mathrm{UT}_{n-i}(n,F)$ for all i by induction on n. The case $n = 1$ is clear. The key to our argument are the following two useful observations:

- If $f : G \longrightarrow H$ is a surjective homomorphism of groups then $f(\mathfrak{z}_i(G)) \subseteq \mathfrak{z}_i(H)$ for all i (first show it for $i = 1$ and then use induction on i).

- If $f : G \longrightarrow H$ is a surjective homomorphism of groups such that $\mathfrak{z}_k(G) \subseteq \ker f$ then $f(\mathfrak{z}_i(G)) \subseteq \mathfrak{z}_{i-k}(H)$ for all i. (The assumptions imply that f factors to a homomorphism $f : G/\mathfrak{z}_k(G) \longrightarrow H$. Since $\mathfrak{z}_i(G)/\mathfrak{z}_k(G)) = \mathfrak{z}_{i-k}(G/\mathfrak{z}_k(G))$, the result follows from our first observation).

Note now that $\mathrm{UT}_{n-i}(n,F)$ is contained both in the kernel of ϕ and ψ and therefore so is the center $\mathfrak{z}_1(\mathrm{UT}(n,F))$. By our second observation, both ϕ and ψ map $\mathfrak{z}_i(\mathrm{UT}(n,F))$ into $\mathfrak{z}_{i-1}(\mathrm{UT}(n-1,F))$, which is contained in $\mathrm{UT}_{n-i}(n-1,F)$ by the inductive assumption. Directly from the definition of ψ and ϕ we see that if $\psi(A)$ and $\phi(A)$ are in $\mathrm{UT}_{n-i}(n-1,F)$ for some $A \in \mathrm{UT}(n,F)$ then $A \in \mathrm{UT}_{n-i}(n,F)$. It follows that $\mathfrak{z}_i(\mathrm{UT}(n,F)) \subseteq \mathrm{UT}_{n-i}(n,F)$ for all i.

d) Describe the centralizer of $\mathrm{UT}_i(n,F)$ in $\mathrm{UT}(n,F)$.

Solution. Let us first make the following general observation.

An $n\times n$ matrix $A=(a_{i,j})$ commutes with $E_{s,t}(a)$, $a\neq 0$, iff $a_{t,l}=0$ for all $l\neq s$, $a_{l,s}=0$ for all $l\neq t$ and $a_{s,s}=a_{t,t}$.

Indeed, the matrices A, $E_{s,t}(a)A$, and $AE_{s,t}(a)$ have the same entries outside the s-th row and t-th column. The s,l entry of $E_{s,t}(a)A$ is $a_{s,l}+aa_{t,l}$ and the m,t entry of this matrix is $a_{m,t}$ for all $m\neq s$. Likewise, the l,t entry of $AE_{s,t}(a)$ equals $aa_{l,s}+a_{l,t}$ and the s,m entry of this matrix is $a_{s,m}$ for $m\neq t$. Comparing the corresponding entries of $E_{s,t}(a)A$ and $AE_{s,t}(a)$ yields our claim.

Recall now that we have seen in the solution to Problem 6 of the first assignment that $\mathrm{UT}_k(n,F)$ is generated by the matrices $E_{s,t}(a)$ with $t-s\geq k$. Thus the centralizer of this group coincides with the set of matrices which commute with all $E_{s,t}(a)$ such that $t-s\geq k$. Our general observation implies now easily that the centralizer of $\mathrm{UT}_k(n,F)$ is the set of matrices $A=(a_{i,j})\in \mathrm{UT}(n,F)$ such that $a_{i,j}=0$ if $k<i<j$ or $i<j\leq n-k$.

Problem 2. a) Let G be any group. Prove that $G^{(i)}\subseteq \gamma_{2^i}(G)$ for all i.

Solution. Recall that $[\gamma_i(G),\gamma_j(G)]\subseteq \gamma_{i+j}(G)$ for all positive integers i,j. Now the result follows by easy induction. Indeed, it is trivially true for $i=1$ and if $G^{(i)}\subseteq \gamma_{2^i}(G)$ then

$$G^{(i+1)}=[G^{(i)},G^{(i)}]\subseteq[\gamma_{2^i}(G),\gamma_{2^i}(G)]\subseteq \gamma_{2^{i+1}}(G).$$

b) Let P be a finite p-group such that $P^{(k)}\neq 1$. Prove that $|P|\geq p^{2^k+k}$.

Solution. Recall the following theorem from class:

Let P be a finite p-group and let $Q\triangleleft P$ be a non-abelian subgroup of $\gamma_k(P)$. Then $|Q/[Q,Q]|\geq p^{k+1}$.

For $k<i\leq 0$ the group $P^{(i)}$ is non-abelian and contained in $\gamma_{2^i}(P)$ (by part a)). Thus by the theorem cited above we have $|P^{(i)}/P^{(i+1)}|\geq p^{2^i+1}$. Clearly $|P^{(k)}|\geq p$. Hence

$$|P|=|P^{(k)}|\prod_{i=0}^{k-1}|P^{(i)}/P^{(i+1)}|\geq p\prod_{i=0}^{k-1}p^{2^i+1}=p^{2^k+k}.$$

Problem 3. Let P be a finite non-abelian p-group such that every proper subgroup of P is abelian. Prove that P is one of the following groups:

1. the quaternion group of order 8;
2. the semidirect product $A\rtimes B$, where $A=<a>$ is a cyclic group of order $p^m\geq p^2$, $B=<b>$ is a cyclic group and $b^{-1}ab=a^{1+p^{m-1}}$;

3. $< a, b : a^{p^m} = b^{p^k} = [a, b]^p = 1, [a, b, a] = 1 = [a, b, b] >$.

Hint. Consider elements a, b in P which do not commute and such that the sum of the orders of a and b is smallest possible.

Solution. We make the following general observation: if $< x, y >$ is a 2-generated group such that $[x, y]$ is central then every element of $< x, y >$ can be written in the form $x^u y^v [x, y]^w$ for some integers u, v, w. In fact, note that

$$(x^u y^v [x, y]^w)(x^p y^q [x, y]^r) = x^u y^v x^p y^q [x, y]^{w+r} = x^u x^p y^v [y^v, x^p] y^q [x, y]^{w+r} =$$

$$= x^{u+p} y^v [y, x]^{vp} y^q [x, y]^{w+r} = x^{u+p} y^{v+q} [x, y]^{w+r-vp}.$$

It follows that elements of the form $x^u y^v [x, y]^w$ form a subgroup and since both $x = x^1 y^0 [x, y]^0$, $y = x^0 y^1 [x, y]^0$ belong to this subgroup, it must be the whole group $< x, y >$.

Consider now the group $G =< a, b : a^{p^m} = b^{p^k} = [a, b]^p = 1, [a, b, a] = 1 = [a, b, b] >$. Our observation above implies that every element of this group can be written in the form $a^u b^v [a, b]^w$, where $0 \leq u < p^m$, $0 \leq v < p^k$, $0 \leq w < p$. Thus G has at most p^{m+n+1} elements. On the other hand, the set $H = \{(u, v, w) : 0 \leq u < p^m,\ 0 \leq v < p^k,\ 0 \leq w < p\}$ with multiplication defined by

$$(u, v, w)(p, q, r) = (u + p, v + q, w + r - vp),$$

where the operations on first coordinates are modulo p^m, on the second coordinate are modulo p^k and on the third coordinate are modulo p, is a group of order p^{m+k+1} with generators $a = (1, 0, 0)$, $b = (0, 1, 0)$ of order p^m, p^k respectively, such that $[a, b] = (0, 0, 1)$ is central and of order p. Thus this group is a homomorphic image of G, and since the $|H| \geq |G|$, G and H are isomorphic. (Alternatively, consider the group $A =< a > \times < c >$, where a has order p^m and c has order p. There is an automorphism f of order p of A such that $f(a) = ac$ and $f(c) = c$. The cyclic group $< b >$ of orderp^k has a homomorphism into the automorphisms of A which sends b to f^{-1}. The corresponding semidirect product $A \rtimes < b >$ has order p^{m+k+1}, is generated by a, b and $[a, b] = c$ has order p and is central. Thus G is isomorphic to $A \rtimes < b >$).

Note that the commutator subgroup of G is generated by conjugates of $[a, b]$, hence it is cyclic of order p and central. For any $x, y \in G$ we have $[x^p, y] = [x, y]^p = 1$, so G^p is central. It follows that $\mathrm{Frat}G = G^p[G, G]$ is central. If M is a maximal subgroup of G then $M/\mathrm{Frat}G$ is cyclic of order p. Since $\mathrm{Frat}G$ is central, we conclude that M is abelian. This shows that every proper subgroup of G is abelian.

Note that the semidirect product $A \rtimes B$, where $A =< a >$ is a cyclic group of order $p^m \geq p^2$, $B =< b >$ is a cyclic group of order p^k and $b^{-1}ab = a^{1+p^{m-1}}$ has generators a, b such that $[a, b] = a^{p^{m-1}}$ is central and of order p. Thus $A \rtimes B$ is a homomorphic image of G and therefore every proper subgroup of it is abelian. It is clear that every proper subgroup of the quaternion group of order 8 is abelian. This shows that the groups listed in the problem have all proper subgroups abelian.

Suppose now that P is a non-abelian p-group with all proper subgroups abelian. We make several observations about P. Suppose that $a, b \in P$ do not commute. Then the subgroup generated by a, b is not abelian, so must be equal to P. Thus

1. P is 2-generated and any two non-commuting elements in P generate P.

Let a, b be generators of P. Note that the subgroup $< a, [a, b] >$ is proper (otherwise P would be cyclic), so a commutes with $[a, b]$. Same argument shows that b commutes with $[a, b]$. Thus $[a, b]$ is cental. Since $\gamma_2(P)$ is generated by conjugates of $[a, b]$ we get

2. $\gamma_2(P)$ is contained in the center of P and therefore P has class 2.

Observe now that for any $x \in P$ the subgroup $< x^p, a >$ is proper (otherwise, since $x^p \in \mathrm{Frat}P$, we would have $P/\mathrm{Frat}P$ is cyclic, and therefore also P would be cyclic). Thus x^p commutes with a. Likewise, x^p commutes with b, so x^p is central. This shows that P^p is central. Since $\mathrm{Frat}P = \gamma_2(P)P^p$, we get

3. $\mathrm{Frat}P$ is contained in the center of P.

Note that $b^{-1}ab = a[a,b]$, so $a^p = b^{-1}a^pb = a^p[a,b]^p$ (since $[a,b]$ and a^p are central). Thus $[a,b]^p = 1$, which implies that

4. $\gamma_2(P)$ is cyclic of order p.

The group $P/\gamma_2(P)$ is abelian, 2-generated but not cyclic. Thus $P/\gamma_2(P)$ is of the form $< \overline{a} > \times < \overline{b} >$(i.e. a product of two cyclic groups). We may choose our generators a, b of P such that $\overline{a}$, $\overline{b}$ are images of a, b in $P/\gamma_2(P)$ (since $\gamma_2(P)$ is a subgroup of $\mathrm{Frat}(P)$). Let the orders of a, b be p^m, p^k respectively. We may assume that $m \geq k$. Since $[a,b]$ is central and has order p, the group P is a homomorphic image of $G =< a, b : a^{p^m} = b^{p^k} = [a,b]^p = 1, [a,b,a] = 1 = [a,b,b] >$.

Suppose now that neither $< a >$ nor $< b >$ contain $[a,b]$. Then the orders of $\overline{a}$, $\overline{b}$ are p^m, p^k respectively. It follows that $P/\gamma_2(P)$ has order p^{m+k}, so $|P| = p^{m+k+1} = |G|$. Thus P is isomorphic to G.

Suppose that $[a,b] \in< a >$ but $[a,b] \notin< b >$. Thus $< a >$ is a normal subgroup of P. Furthermore, $[a,b] = a^{p^{m-1}l}$ for some l prime to p. There is d such that $p|(dl-1)$ and then $[a,b^d] = a^{p^{m-1}}$. Replacing b by b^d we may assume that $[a,b] = a^{p^{m-1}}$. Note that $< a > \cap < b >= 1$ (any element in this intersection must be trivial in $P/\gamma_2(P)$, so belongs to $\gamma_2(P) =< [a,b] >$). It follows that P is the semidirect product $A \rtimes B$, where $A =< a >$ is a cyclic group of order $p^m \geq p^2$, $B =< b >$ is a cyclic group and $b^{-1}ab = a^{1+p^{m-1}}$.

Suppose now that both $< a >$ and $< b >$ contain $[a,b]$. Thus $[a,b] = a^{p^{m-1}n} = b^{p^{k-1}l}$ for some l, n prime to p. If p is odd then P is regular (since it has class 2) so $(a^{p^{m-k}n}b^{-l})^{p^{k-1}} = 1$. If $p = 2$ then $(xy)^2 = x^2y^2[y,x]$ (since $[x,y]$ is central) for any $x, y \in P$. Recall that x^2 and y^2 are central and therefore $(xy)^{2^j} = x^{2^j}y^{2^j}$ for any $x, y \in P$ and any $j \geq 2$. If $m > k$ then $a^{p^{m-k}n}$ is central and again $(a^{p^{m-k}n}b^{-l})^{p^{k-1}} = 1$. If $m = k > 2$ then again $(a^{p^{m-k}n}b^{-l})^{p^{k-1}} = 1$. In all these cases the order of $\overline{b}^{-l}$ is p^{k-1}, so the order of $\overline{a}^{p^{m-k}n}\overline{b}^{-l}$ is at lest p^{k-1} ant therefore the element $b' = a^{p^{m-k}n}b^{-l}$ has order exactly p^{k-1} and $[a,b]$ does not belong to $< b' >$. Clearly a and b' generate P and replacing b by b' we arrive at the case already considered, in which P is the semidirect product $A \rtimes B$, where $A =< a >$ is a cyclic group of order $p^m \geq p^2$, $B =< b >$ is a cyclic group and $b^{-1}ab = a^{1+p^{m-1}}$.

It remains to consider the case when $p = 2$, $k = m = 2$ and both $< a >$, $< b >$ contain $[a,b]$. Thus P is a non-abelian group of order 8 with two distinct cyclic subgroups of order 4, so P is the quaternion group of order 8.

Problem 4. Let G be a group generated by a set S.

a) Show that $\gamma_k(G)$ is generated by the set $\{[x_1, ..., x_k]^g : x_i \in S \text{ for } i = 1, 2, ..., k \text{ and } g \in G\}$.

Solution. Let G_k be the subgroup of G generated by the set $\{[x_1, ..., x_k]^g : x_i \in S \text{ for } i = 1, 2, ..., k \text{ and } g \in G\}$. Clearly $G_k \triangleleft G$. Since $[x_1, ..., x_k]^g = [x_1^g, ..., x_k^g] \in \gamma_k(G)$, we have $G_k \subseteq \gamma_k(G)$.

Suppose that $G_k = \gamma_k(G)$ for some k. Consider the group G/G_{k+1}. For $a \in G$ we denote by $\overline{a}$ the image of a in G/G_{k+1}. Note that $[\overline{x}_1, ..., \overline{x}_k, \overline{x}_{k+1}] = \overline{[x_1, ..., x_{k+1}]} = 1$ for any $x_i \in S$. It follows that $[\overline{x}_1, ..., \overline{x}_k]$ commutes with $\overline{x}$ for all $x \in S$. But the elements $\overline{x}$, $x \in S$, generate G/G_{k+1}. Thus $[\overline{x}_1, ..., \overline{x}_k]$ is central in G/G_{k+1} for any $x_i \in S$. Since the center is a normal subgroup, we have $\overline{[x_1, ..., x_k]^g} = [\overline{x}_1, ..., \overline{x}_k]^{\overline{g}}$ is central for all $x_i \in S$ and all $g \in G$. This shows that the image of G_k in G/G_{k+1} is central. Thus

$$\gamma_{k+1}(G) = [\gamma_k(G), G] = [G_k, G] \subseteq G_{k+1} \subseteq \gamma_{k+1}(G),$$

so $\gamma_{k+1}(G) = G_{k+1}$. The result follows then by induction on k.

b) Prove that $\gamma_k(G)$ is generated by the set $\{[x_1, ..., x_k] : x_i \in S \text{ for } i = 1, 2, ..., k\} \cup \gamma_{k+1}(G)$.

Solution. Note that $[x_1, ..., x_k]^g = [x_1, ..., x_k][x_1, ..., x_k, g]$ and $[x_1, ..., x_k, g] \in \gamma_{k+1}(G)$. Thus the group generated by the set $\{[x_1, ..., x_k] : x_i \in S \text{ for } i = 1, 2, ..., k\} \cup \gamma_{k+1}(G)$ contains the set $\{[x_1, ..., x_k]^g : x_i \in S \text{ for } i = 1, 2, ..., k \text{ and } g \in G\}$, hence also the subgroup generated by this set, which by a) equals $\gamma_k(G)$. Since the reversed inclusion is clearly true (i.e. the group generated by the set $\{[x_1, ..., x_k] : x_i \in S \text{ for } i = 1, 2, ..., k\} \cup \gamma_{k+1}(G)$ is contained in $\gamma_k(G)$), the result follows.

c) Show that if G is generated by two elements then $\gamma_2(G)/\gamma_3(G)$ is cyclic.

Solution. Let x, y generate G. Thus by b), the group $\gamma_2(G)$ is generated by $\{[x, x], [x, y], [y, x], [y, y]\} \cup \gamma_3(G)$. Since $[x, x] = [y, y] = 1$ and $[y, x] = [x, y]^{-1}$, the group $\gamma_2(G)$ is generated by $\{[x, y]\} \cup \gamma_3(G)$. Thus the factor group $\gamma_2(G)/\gamma_3(G)$ is generated by the image of $[x, y]$, so it is cyclic.

d) Show that if $a_i \in \gamma_{m_i}(G)$ then $[a_1^{k_1}, a_2^{k_2}, ..., a_s^{k_s}] \equiv [a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s} \mod \gamma_{1+m_1+m_2+...+m_s}(G)$.

Solution. Note first that if $a \in \gamma_m(G)$ and $b \in \gamma_n(G)$ then $[a, b] \in \gamma_{m+n}(G)$. Thus $[a, [a, b]]$ and $[b, [a, b]]$ are in $\gamma_{m+n+1}(G)$. In other words, in the group $G/\gamma_{m+n+1}(G)$ the elements $\overline{a}, \overline{b}$ commute with $\overline{[a, b]} = [\overline{a}, \overline{b}]$. Thus $[\overline{a}^k, \overline{b}^l] = \overline{a}, \overline{b}]^{kl}$. This is equivalent to $[a^k, b^l] \equiv [a, b]^{kl}$ mod $\gamma_{1+m+n}(G)$. We have therefore established the result for $s = 2$.

Now we proceed by induction on s. Assuming the result for s we may write $[a_1^{k_1}, a_2^{k_2}, ..., a_s^{k_s}] = [a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s} w$ for some $w \in \gamma_{1+m_1+m_2+...+m_s}(G)$. Thus

$$[a_1^{k_1}, a_2^{k_2}, ..., a_s^{k_s}, a_{s+1}^{k_{s+1}}] = [[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s} w, a_{s+1}^{k_{s+1}}] =$$

$$= [[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s}, a_{s+1}^{k_{s+1}}][[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s}, a_{s+1}^{k_{s+1}}, w][w, a_{s+1}^{k_{s+1}}].$$

Note that $[a_1, a_2, ..., a_s] \in \gamma_{m_1+m_2+...+m_s}(G)$. Thus

$$[[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s}, a_{s+1}^{k_{s+1}}, w] \in \gamma_{m_1+m_2+...+m_s+m_{s+1}+1+m_1+m_2+...+m_s}(G) \subseteq \gamma_{1+m_1+m_2+...+m_s+m_{s+1}}(G)$$

and $[w, a_{s+1}^{k_{s+1}}] \in \gamma_{1+m_1+m_2+...+m_s+m_{s+1}}(G)$. Hence

$$[[a_1^{k_1}, a_2^{k_2}, ..., a_s^{k_s}, a_{s+1}^{k_{s+1}}] \equiv [[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s}, a_{s+1}^{k_{s+1}}] \mod \gamma_{1+m_1+m_2+...+m_s+m_{s+1}}(G).$$

Since $[a_1, a_2, ..., a_s]\gamma_{m_1+m_2+...+m_s}(G)$, the case $s = 2$ (which we have established) implies that

$$[[a_1, a_2, ..., a_s]^{k_1 k_2 ... k_s}, a_{s+1}^{k_{s+1}}] \equiv [[a_1, a_2, ..., a_s], a_{s+1}]^{k_1 k_2 ... k_s k_{s+1}} =$$

$$= [a_1, a_2, ..., a_s, a_{s+1}]^{k_1 k_2 ... k_s k_{s+1}} \mod \gamma_{1+m_1+m_2+...+m_s+m_{s+1}}(G),$$

and this proves the result for $s + 1$.

Problem 5. Show that $(xy)^3 \equiv x^3y^3[y,x]^3[y,x,x][y,x,y]^5 \mod \gamma_4(G)$ for any group G and any $x, y \in G$.

Solution. Suppose that $\gamma_4(G) = 1$. Then $\gamma_2(G)$ is abelian (since $[\gamma_2, \gamma_2] \subseteq \gamma_4$). Note that

$$yxyx = xy[y,x]xy[y,x] = xyx[y,x][y,x,x]y[y,x] = xxy[y,x][y,x][y,x,x]y[y,x] =$$

$$= x^2y[y,x][y,x]y[y,x][y,x,x] = x^2y[y,x]y[y,x][y,x,y][y,x][y,x,x] =$$
$$= x^2yy[y,x][y,x,y][y,x][y,x,y][y,x][y,x,x] = x^2y^2[y,x]^3[y,x,x][y,x,y]^2.$$

Thus

$$x^3y^3 = x(yxyx)y = xx^2y^2[y,x]^3[y,x,x][y,x,y]^2y = x^3y^2[y,x]^3y[y,x,x][y,x,y]^2 =$$

$$= x^3y^2[y,x][y,x]y[y,x][y,x,y][y,x,x][y,x,y]^2 = x^3y^2[y,x]y[y,x][y,x,y][y,x][y,x,x][y,x,y]^3 =$$
$$= x^3y^2y[y,x][y,x,y][y,x]^2[y,x,x][y,x,y]^4 = x^3y^3[y,x]^3[y,x,x][y,x,y]^5$$

Problem 6. Let P be a regular p-group of exponent p^k such that the subgroup $\Omega_{k-1}(P)$ is maximal. Show that P is generated by a set of elements of order exactly p^k. Prove that there is no finite p-group H such that P is isomorphic to $H/Z(H)$.

Solution. Note that an element of P has order p^k iff it does not belong to $\Omega_{k-1}(P)$. If P has order p^n then $\Omega_{k-1}(P)$ has order p^{n-1} and therefore there are $p^n - p^{n-1} \geq p^{n-1}$ elements of order p^k. The subgroup generated by these elements has at least $p^{n-1}+1$ elements (the trivial element is not in the generating set), so it must be the whole group P.

Since P is regular, we have $|P| = |\Omega_{k-1}(P)||P^{p^{k-1}}|$. Thus $P^{p^{k-1}}$ is cyclic of order p. Let a be a generator of $P^{p^{k-1}}$. Note that if $g \notin \Omega_{k-1}(P)$ then $g^{p^{k-1}} = a^l$ for some l prime to p.

Suppose that $f : H \longrightarrow P$ is a surjective homomorphism such that H is a p-group and $\ker f$ is the center of H. Chose any $u \in H$ such that $f(u) = a$. If $h \in H$ is such that $f(h) \notin \Omega_{k-1}(P)$ then $f(h^{p^{k-1}}) = f(h)^{p^{k-1}} = a^l = f(u^l)$ for some l prime to p. Thus $u^l = h^{p^{k-1}}z$ for some z in the center of H. It follows that h commutes with u^l. Since l is prime to p, we have $< u >=< u^l >$ and consequently h commutes with u. If $g \in H$ is such that $f(g) \in \Omega_{k-1}(P)$ then $f(hg) \notin \Omega_{k-1}(P)$. Thus both h and hg commute with u and therefore g also commutes with u. This means that every element of H commutes with u, so $u \in Z(H) = \ker f$. This is however not possible since $f(u) = a \neq 1$.