GROUP THEORY EXERCISES AND SOLUTIONS

Mahmut Kuzucuoğlu
Middle East Technical University
matmah@metu.edu.tr
Ankara, TURKEY

December 12, 2014

TABLE OF CONTENTS

CHAPTERS

Preface

I have given some group theory courses in various years. These problems are given to students from the books which I have followed that year. I have kept the solutions of exercises which I solved for the students. These notes are collection of those solutions of exercises.

Mahmut Kuzucuoğlu
METU, Ankara
December 12, 2014

GROUP THEORY EXERCISES AND SOLUTIONS

M. Kuzucuoğlu

1. SEMIGROUPS

Definition A semigroup is a nonempty set S together with an associative binary operation on S. The operation is often called multiplication and if $x, y \in S$ the product of x and y (in that ordering) is written as xy.

1.1. *Give an example of a semigroup without an identity element.*

Solution $\mathbb{Z}^+ = \{1, 2, 3, ...\}$ is a semigroup without identity with binary operation usual addition.

1.2. *Give an example of an infinite semigroup with an identity element e such that no element except e has an inverse.*

Solution $\mathbb{N} = \{0, 1, 2, ...\}$ is a semigroup with binary operation usual addition. No non-identity element has an inverse.

1.3. *Let S be a semigroup and let $x \in S$. Show that $\{x\}$ forms a subgroup of S (of order 1) if and only if $x^2 = x$ such an element x is called idempotent in S.*

Solution Assume that $\{x\}$ forms a subgroup. Then $\{x\} \cong \{1\}$ and $x^2 = x$.

Conversely assume that $x^2 = x$. Then associativity is inherited from S. So Identity element of the set $\{x\}$ is itself and inverse of x is also itself. Then $\{x\}$ forms a subgroup of S.

2. GROUPS

Let V be a vector space over the field F. The set of all linear invertible maps from V to V is called **general linear group** of V and denoted by $GL(V)$.

2.1. *Suppose that F is a finite field with say $|F| = p^m = q$ and that V has finite dimension n over F. Then find the order of $GL(V)$.*

Solution Let F be a finite field with say $|F| = p^m = q$ and that V has finite dimension n over F. Then $|V| = q^n$ for any base $w_1, w_2, ..., w_n$ of V, there is unique linear map $\theta : V \to V$ such that $v_i\theta = w_i$ for $i = 1, 2, ..., n$.
Hence $|GL(V)|$ is equal to the number of ordered bases of V, in forming a base $w_1, w_2, ..., w_n$ of V we may first choose w_1 to be any nonzero vector of V then w_2 be any vector other than a scalar multiple of w_1. Then w_3 to be any vector other than a linear combination of w_1 and w_2 and so on. Hence
$|GL(V)| = (q^n - 1)(q^n - q)(q^n - q^2)....(q^n - q^{n-1})$.

2.2. *Let G be the set of all matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ where a, b, c are real numbers such that $ac \neq 0$.*
(a) Prove that G forms a subgroup of $GL_2(\mathbb{R})$.

Indeed

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \in G$$

$ac \neq 0, df \neq 0$, implies that $acdf \neq 0$ for all $a, c, d, f \in \mathbb{R}$. Since determinant of the matrices are all non-zero they are clearly invertible.
(b) The set H of all elements of G in which $a = c = 1$ forms a subgroup of G isomorphic to $\mathbb{R}^+$. Indeed $H = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \}$

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} \in H. \text{ So } H \leq G.$$

Moreover $H \cong \mathbb{R}^+$

$$\begin{aligned} \varphi : H &\rightarrow \mathbb{R}^+ \\ \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} &\rightarrow b_1 \end{aligned}$$

$$\varphi[\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}] = b_1 + b_2 = \varphi\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\varphi\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}$$

$Ker\varphi = \{\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \mid \varphi\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} = 0 = b_1\} = Id$. So φ is one-to-one.

Then for all $b \in \mathbb{R}$, there exists $h \in H$ such that $\varphi(h) = b$, where $h = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Hence φ is an isomorphism.

2.3. *Let $\alpha \in Aut\ G$ and let $H = \{g \in G : g^\alpha = g\}$. Prove that H is a subgroup of G, it is called the fixed point subgroup of G under α.*

Solution Let $g_1, g_2 \in H$. Then $g_1^\alpha = g_1$ and $g_2^\alpha = g_2$. Now
$(g_1g_2)^\alpha = g_1^\alpha g_2^\alpha = g_1g_2$
$(g_2^{-1})^\alpha = (g_2^\alpha)^{-1} = g_2^{-1} \in H$. So H is a subgroup.

2.4. *Let n be a positive integer and F a field. For any $n \times n$ matrix y with entries in F let y^t denote the transpose of y. Show that the map*

$$\begin{aligned} \phi : GL_n(F) &\rightarrow GL_n(F) \\ x &\rightarrow (x^{-1})^t \end{aligned}$$

for all $x \in GL_n(F)$ is an automorphism of $GL_n(F)$ and that the corresponding fixed point subgroup consist of all orthogonal $n \times n$ matrices with entries in F. (That is matrices y such that $y^ty = 1$)

Solution

$$\begin{aligned}\phi(x_1x_2) &= [(x_1x_2)^{-1}]^t \\ &= [x_2^{-1}x_1^{-1}]^t \\ &= (x_1^{-1})^t(x_2^{-1})^t = \phi(x_1)\phi(x_2)\end{aligned}$$

Now if $\phi(x_1) = 1 = (x_1^{-1})^t$, then $x_1^{-1} = 1$. Hence $x_1 = 1$. So ϕ is a monomorphism. For all $x \in GL_n(F)$ there exists $x_1 \in GL_n(F)$ such that $\phi(x_1) = x$. Let $x_1 = (x^{-1})^t$. So we obtain ϕ is an automorphism. Let $H = \{x \in GL_n(F) : \phi(x) = x\}$. We show in the previous exercise that H is a subgroup of $GL_n(F)$. Now for $x \in H$ $\phi(x) = x = (x^{-1})^t$ implies $xx^t = 1$. That is the set of the orthogonal matrices.

Recall that if $G = G_1 \times G_2$, then the subgroup H of G may not be of the form $H_1 \times H_2$ as $H = \{(0,0),(1,1)\}$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ but H is not of the form $H_1 \times H_2$ where H_i is a subgroup of G_i. But the following question shows that if $|G_1|$ and $|G_2|$ are relatively prime, then every subgroup of G is of the form $H_1 \times H_2$.

2.5. *Let $G = G_1 \times G_2$ be a finite group with* $\gcd(|G_1|, |G_2|)) = 1$. *Then every subgroup H of G is of the form $H = H_1 \times H_2$ where H_i is a subgroup of G_i for $i = 1, 2$.*

Solution: Let H be a subgroup of G. Let π_i be the natural projection from G to G_i. Then the restriction of π_i to H gives homomorphisms from H to G_i for $i = 1, 2$. Let $H_i = \pi_i(H)$ for $i = 1, 2$. Then clearly $H \leq H_1 \times H_2$ and $H_i \leq G_i$ for $i = 1, 2$. Then $H/Ker(\pi_1) \cong H_1$ implies that $|H_1| \mid |H|$ similarly $|H_2| \mid |H|$. But $\gcd(|H_1|, |H_2|) = 1$ implies that $|H_1||H_2| \mid |H|$. So $H = H_1 \times H_2$.

2.6. *Let $H \trianglelefteq G$ and $K \trianglelefteq G$. Then $H \cap K \trianglelefteq G$. Show that we can define a map*

$$\begin{aligned}\varphi \ &: \ G/H \cap K \longrightarrow G/H \times G/K \\ &\quad g(H \cap K) \longrightarrow (gH, gK)\end{aligned}$$

for all $g \in G$ and that φ is an injective homomorphism. Thus $G/(H \cap K)$ can be embedded in $G/H \times G/K$. Deduce that if G/H and G/K or both abelian, then $G/H \cap K$ abelian.

Solution As H and K are normal in G, clearly $H \cap K$ is normal in G.
$\varphi : G/H \cap K \longrightarrow G/H \times G/K$

$$\begin{aligned}\varphi(g(H\cap K)g'(H\cap K)) &= \varphi(gg'(H\cap K))\\ &= (gg'H, gg'K)\\ &= (gH, gK)(g'H, g'K)\\ &= \varphi(g(H\cap K))\varphi(g'(H\cap K)).\end{aligned}$$

So φ is an homomorphism. $Ker\varphi = \{g(H\cap K) : \varphi(g(H\cap K)) = (\bar{e},\bar{e}) = (gH, gK)\}$. Then $g \in H$ and $g \in K$ implies that $g \in H\cap K$. So $Ker\varphi = H\cap K$. If G/H and G/K are abelian, then $g_1Hg_2H = g_1g_2H = g_2g_1H$. Similarly $g_1g_2K = g_2g_1K$ for all $g_1, g_2 \in G$, $g_2^{-1}g_1^{-1}g_2g_1 \in H$, $g_2^{-1}g_1^{-1}g_2g_1 \in K$. So for all $g_1, g_2 \in G$, $g_2^{-1}g_1^{-1}g_2g_1 \in H \cap K$. $g_2^{-1}g_1^{-1}g_2g_1(H\cap K) = H \cap K$. So $g_2g_1(H\cap K) = g_1g_2(H\cap K)$.

2.7. *Let G be finite non-abelian group of order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not a simple group.*

Solution Let $|G| = n$ and p be the smallest prime dividing $|G|$. If G is a p-group, then $1 \neq Z(G) \lneqq G$. Hence G is not simple. So we may assume that G has composite order. Then by assumption G has a subgroup M of index p in G. i.e. $|G : M| = p$. Then G acts on the right cosets of M by right multiplication. Hence there exists a homomorphism $\phi : \quad G \hookrightarrow Sym(\text{p})$. Then $G/Ker\phi$ is isomorphic to a subgroup of $Sym(\text{p})$. Since p is the smallest prime dividing the order of G we obtain $|G/Ker\phi| |\, p!$ which implies that $|G/Ker\phi| = p$. Hence $Ker\phi \neq 1$ otherwise $Ker\ \phi = 1$ implies that G is abelian and isomorphic to Z_p. But by assumption G is non-abelian.

2.8. *Let $M \leq N$ be normal subgroups of a group G and H a subgroup of G such that $[N, H] \leq M$ and $[M, H] = 1$. Prove that for all $h \in H$ and $x \in N$*

(i) $[h, x] \in Z(M)$

(ii) *The map*

$$\begin{aligned} \theta_x : H &\to Z(M) \\ h &\to [h,x] \end{aligned}$$

is a homomorphism.

(iii) *Show that $H/C_H(N)$ is abelian.*

Solution: Let $h \in H$ and $x \in N$. Then $[h,x] = h^{-1}x^{-1}hx \in [N,H] \leq M$. Moreover for any $m \in M$, we need to show $m[h,x] = [h,x]m$ if and only if $m^{-1}h^{-1}x^{-1}hxm = h^{-1}x^{-1}hx$ if and only if
$m^{-1}h^{-1}x^{-1}hxmx^{-1}h^{-1}xh = 1$ if and only if $m^{-1}h^{-1}x^{-1}(xmx^{-1})hh^{-1}xh = 1$. That is true as $mh = hm$ and M is normal in G we have, $xmx^{-1} \in M$ and $xmx^{-1}h = hxmx^{-1}$

(ii)

$$\begin{aligned} \theta_x(h_1h_2) &= [h_1h_2, x] \\ &= [h_1,x]^{h_2}[h_2,x] \\ &= [h_1,x][h_2,x] \end{aligned}$$

as $[h_1,x] \in Z(M)$ and so $h_2^{-1}mh_2 = m$.

(iii) It is easy to see that $Ker\theta_x = C_H(x)$. Then we can define a map

$$\begin{aligned} \psi : H \to \quad & Z(M)\times \quad Z(M) \times \ldots \times Z(M) \ldots \\ h \to \quad & [h,x_1]\times \quad [h,x_2] \times \ldots \times [h,x_i] \ldots \end{aligned}$$

where all $x_j \in N$. Then the kernel of ψ is $\underset{x_j \in N}{\cap} C_H(x_j) = C_H(N)$. Then the map from $H/C_H(N)$ to the right hand side is into and the right hand side is abelian we have $H/C_H(N)$ is abelian.

2.9. *Let G be a finite group and $\Phi(G)$ the intersection of all maximal subgroups of G. Let N be an abelian minimal normal subgroup of G. Then N has a complement in G if and only if $N \ntrianglelefteq \Phi(G)$*

Solution Assume that N has a complement H in G. Then $G = NH$ and $N \cap H = 1$. Since G is finite there exists a maximal subgroup $M \geq H$. Then N is not in M which implies N is not in $\Phi(G)$. Because, if $N \leq M$, then $G = HN \leq M$ which is a contradiction.

Conversely assume that $N \nleq \Phi(G)$. Then there exists a maximal subgroup M of G such that $N \nleq M$. Then by maximality of M we have $G = NM$. Since N is abelian N normalizes $N \cap M$ hence $G = NM \leq N_G(N \cap M)$ i.e. $N \cap M$ is an abelian normal subgroup of G. But minimality of N implies $N \cap M = 1$. Hence M is a complement of N in G.

2.10. *Show that $F(G/\phi(G)) = F(G)/\phi(G)$.*

Solution: **(i)** $F(G)/\phi(G)$ is nilpotent normal subgroup of $G/\phi(G)$ so $F(G)/\phi(G) \leq F(G/\phi(G))$.
Let $K/\phi(G) = F(G/\phi(G))$. Then $K/\phi(G)$ is maximal normal nilpotent subgroup of $G/\phi(G)$. In particular $K \trianglelefteq G$ and $K/\phi(G)$ is nilpotent. It follows that K is nilpotent in G. This implies that $K \leq F(G)$. $K/\phi(G) \leq F(G)/\phi(G)$ which implies $F(G/\phi(G)) = F(G)/\phi(G)$.

2.11. *If $F(G)$ is a p-group, then $F(G/F(G))$ is a p'- group.*

Solution: Let $K/F(G) = F(G/F(G))$, maximal normal nilpotent subgroup of $G/F(G)$. So $K/F(G) = \underset{q\in\Pi(G)}{Dr} \; O_q(K/F(G)) = P_1/F(G) \times P_2/F(G) \times \ldots \times P_m/F(G)$. Since $F(G)$ is a p-group so one of $P_i/F(G)$ is a p-group, say $P_1/F(G)$ is a p-group.

Now P_1 is a p-group, $P_1/F(G) char K/F(G) char G/F(G)$ implies that $P_1/F(G) char G/F(G)$ implies $P_1 \triangleleft G$. This implies P_1 is a p-group and hence nilpotent and normal implies $P_1 \leq F(G)$. So $P_1/F(G) = \overline{id}$ i.e $K/F(G) = F(G/F(G))$ is a p'-group.

Observe this in the following example. S_3, $F(S_3) = A_3$. $F(S_3/A_3) = S_3/A_3 \cong \mathbb{Z}_2$ is a 2-group.

2.12. *Let $G = \{(a_{ij}) \in GL(n,F) \mid a_{ij} = 0 \; if \, i > j \;\; and \;\; a_{ii} = a, \; i = 1\ldots,n\}$ where F is a field, be the group of upper triangular* *matrices all of whose diagonal entries are equal. Prove that* $G \cong D \times U$ *where* D *is the group of all non-zero multiples of the identity matrix and* U *is the group of upper triangular matrices with 1's down diagonal.*

Solution

$$\begin{array}{ccc} \text{d:}\ \ G & \rightarrow & F^* \\ \begin{pmatrix} a & c_{12} & c_{13} & c_{14} & \dots & c_{1n} \\ 0 & a & c_{23} & c_{24} & \dots & c_{2n} \\ & & . & & & \\ & & & . & \dots & * \\ 0 & 0 & 0 & 0 & a & c_{n-1n} \\ 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} & \rightarrow & a \end{array}$$

It is clear that d is a homomorphism and $Ker\ d = U$. So U is normal $D \cap U = 1$. Since F is a field and a is a non-zero element every element $g \in G$ can be written as a product $g = cu$ where $c \in D$ and $u \in U$. So $DU = G$. Moreover D is normal in G in fact D is central in G. So $G = DU \cong D \times U$.

2.13. *Prove that if* N *is a normal subgroup of the finite group* G *and*
$(|N|, |G : N|) = 1$, *then* N *is the unique subgroup of order* $|N|$.

Solution If M is another subgroup of G of order $|N|$. Then NM is a subgroup of G as $N \lhd G$. Now $|NM| = \frac{|N||M|}{|N \cap M|}$. If $N \neq M$, then $|NM| > |N|$ and if π is the set of primes dividing $|N|$, then N is a maximal π-subgroup of G. But MN is also a π-group containing N properly. Hence $MN = N$. i.e $M \leq N$.

2.14. *Let* F *be a field. Define a binary operation* $*$ *on* F *by* $a * b = a + b - ab$ *for all* $a, b \in F$.
Prove that the set of all elements of F *distinct from* 1 *forms a group* $F^x = F \setminus \{1\}$ *with respect to the operation* $*$ *and that* $F^* \cong F^x$ *where* F^* *is the multiplicative group on* $F \setminus \{0\}$ *with respect to the usual multiplication in the field.*

Solution $*$ is a binary operation on F^x as $a+b-ab=1$ implies $(a-1)(1-b)=0$ but $a\neq 1$ and $b\neq 1$ implies image of $*$ is in F^x. Indeed $*$ is a binary operation and $*: F^x\times F^x\to F^x$

(i) associativity of $*$: We need to show $a*(b*c)=(a*b)*c$
Indeed $a*(b*c)=a*(b+c-bc)$ and $(a*b)*c=(a+b-ab)*c$
Then $a*(b*c)= a+b+c-bc-(ab+ac-abc)=a+b-ab+c-ac-bc+abc=(a*b)*c$ So associativity holds.

(ii) For the identity element, let $a*b=a$ for all $a\in F$ implies b is the identity element. The equality implies that $a+b-ab=a$. Hence $b-ab=0$ i.e $b(1-a)=0$. Since this is true for all a and $a\neq 1$ we obtain $b=0$ and 0 is the identity element.

(iii) $a*b=b*a$ if and only if $a+b-ab=b+a-ba$ if and only if $-ab=-ba$ since we are in a field for all $a,b\in F$ we have $ab=ba$. So $a*b=b*a$ for all $a\in F$.

(iv) Now for all $a\in F^{\setminus}\{0\}$, there exists $a'\in F$ such that $a*a'=0$ $=a+a'-aa'$ implies $a+a'=aa'$. So $a'=a(1-a)^{-1}$. Hence F^x is an abelian group with respect to $*$. Let

$$\begin{aligned}\phi: F^x &\to F^*\\ a\to &\quad 1-a\end{aligned}$$

$\phi(a*b)=\phi(a+b-ab)=1-a-b+ab=(1-a)(1-b)=\phi(a)\phi(b)$.
Then $Ker\phi=\{a\in F^x\ :\ \phi(a)=1\}=\{a\in F^x\ :\ 1-a=1\}=\{0\}$.

ϕ is onto as for any $b\in F^*$ so $b\neq 0$, $\phi(x)=b$ implies that $1-x=b$ so $x=1-b$ and $x\neq 1$. Hence ϕ is an isomorphism.

2.15. *Consider the direct square $G\times G$ of G. Let $\hat{G}=\{(g,g): g\in G\}\subseteq G\times G$.*

(i) Show that $\hat{G}$ is a subgroup of $G\times G$ which is isomorphic to G. $\hat{G}$ is called the ***diagonal*** *subgroup of $G\times G$.*

(ii) Show also that $\hat{G}\trianglelefteq G\times G$ if and only if G is abelian.

Solution i) $\hat{G}$ is a subgroup of G. Indeed $(g_1,g_1),(g_2,g_2)\in\hat{G}$. $(g_1,g_1)(g_2,g_2)=(g_1g_2,g_1g_2)\in\hat{G}$. $(g_1^{-1},g_1^{-1})\in\hat{G}$ which implies $\hat{G}$ is a subgroup of $G\times G$.

$\hat{G} \cong G$. Indeed define

$$\begin{aligned} \varphi \ : \ & G \longrightarrow \hat{G} \\ & g \longrightarrow (g, g) \end{aligned}$$

$\varphi(gg') = (gg', gg') = (g, g)(g', g') = \varphi(g)\varphi(g')$. So φ is a homomorphism.

$\varphi(g) = 1 = (g, g)$. This implies $g = 1$. So φ is a monomorphism. For all $(g_i, g_i) \in \hat{G}$ there exists $g_i \in G$ such that $\varphi(g_i) = (g_i, g_i)$. So φ is onto. Hence φ is an isomorphism.

ii) $\hat{G} \trianglelefteq G \times G$ if and only if G is abelian.

Assume $\hat{G}$ is a normal subgroup of $G \times G$. Then for any $g_1, g_2 \in G$,

$(g_1, g_2)^{-1}(x, x)(g_1, g_2) = (g_1^{-1}xg_1, g_2^{-1}xg_2) \in \hat{G}$. In particular $g_1 = 1$ implies for all g_2, and for all $x \in G, g_2^{-1}xg_2 = x$. Hence G is abelian.

Conversely if G is abelian, then $G \times G$ is abelian and every subgroup of $G \times G$ is normal in G, in particular $\hat{G}$ is normal in G.

2.16. *Suppose $H \trianglelefteq G$. Show that if x, y elements in G such that $xy \in H$, then $yx \in H$.*

Solution $H \trianglelefteq G$, implies that every left coset is also a right coset $Hx = xH$, $yH = Hy$, $xy \in H$ so $H = xyH$.
$xH = Hx$ implies $xyxH = xyHx = Hx$. Then $yxH = x^{-1}Hx = H$. Hence $yx \in H$.

2.17. *Give an example of a group such that normality is not transitive.*

Solution Let us consider A_4 alternating group on four letters. Then $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4. Since V is abelian any subgroup of V is a normal subgroup of V. But $H = \{1, (12)(34)\}$ is not normal in A_4.

Another Solution Let's consider $G = S_3 \times S_3$, $A_3 = \{1, (123), (132)\}$. $A_3 \triangleleft S_3$. Let

$A = \{ \ (1, 1), ((123), (123)), ((132), (132)) \ \} \leq G$, A is diagonal subgroup of $A_3 \times A_3$ and $A \cong A_3$. $A \triangleleft A_3 \times A_3 \triangleleft G$. But A is not normal in G as $((12), 1)^{-1}((123), (123))((12), 1) = ((132), (123)) \notin A$.

2.18. *If $\alpha \in AutG$ and $x \in G$, then $|x^\alpha| = |x|$.*

Solution First observe that $(x^\alpha)^n = (x^n)^\alpha$. If x^α has finite order say n, then $(x^\alpha)^n = 1 = (x^n)^\alpha = 1^\alpha$. Hence $x^n = 1$ as α is an automorphism. Hence x has finite order dividing n. If order of x is less than or equal to n, say m. Then we obtain $x^m = 1$. Then $(x^m)^\alpha = 1^\alpha = 1$. Hence $(x^\alpha)^m = 1$. It follows that $n = m$, i.e. $|x^\alpha| = |x|$ when the order is finite. But the above proof shows that if order of x^α is infinite then order of x must be infinite. In particular conjugate elements of a group have the same order. We can consider the semidirect product of G with the $Aut(G)$. Then in the semidirect product the elements x and x^α becomes conjugate elements.

2.19. *Let H and K be subgroups of G and $x, y \in G$ with $Hx = Ky$. Then show that $H = K$.*

Solution $Hx = Ky$ implies $Hxy^{-1} = K$. As H is a subgroup, $1 \in H$ and so $xy^{-1} \in Hxy^{-1} = K$. Then $yx^{-1} \in K$. It follows that $K = Kyx^{-1}$. Then $K = Kxy^{-1} = Kyx^{-1} = H$. Hence $K = H$.

2.20. *Prove that if K is a normal subgroup of the group G, then $Z(K)$ is a normal subgroup of G. Show by an example that $Z(K)$ need not be contained in $Z(G)$.*

Solution: Let $z \in Z(K)$, $k \in K$ and $g \in G$. Then $g^{-1}zg \in K$ as $K \trianglelefteq G$ and $(g^{-1}zg)k(g^{-1}z^{-1}g)k^{-1} = g^{-1}z(gkg^{-1})z^{-1}gk^{-1} = g^{-1}(gkg^{-1})zz^{-1}gk^{-1} = 1$. Hence $Z(K) \trianglelefteq G$.

Now as an example consider A_3 in S_3. $Z(A_3) = A_3$ but $Z(S_3) = 1$.

2.21. *Let $x, y \in G$ and let $xy = z$ if $z \in Z(G)$, then show that x and y commute.*

Solution: $xy = z \in Z(G)$ implies for all $g \in G$, $(xy)g = g(xy)$. This is also true for x, hence $(xy)x = x(xy)$. Now multiply both side by x^{-1}, we obtain $yx = xy$. Then x and y are commute.

2.22. *Let $UT(3, F)$ be the set of all matrices of the form*

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

where a, b, c are arbitrary elements of a field F, moreover 0 and 1 are the zero and the identity elements of F respectively. Prove that
(i) $UT(3,F) \leq GL(3,F)$
(ii) $Z(UT(3,F)) \cong F^+$ and $UT(3,F)/Z(UT(3,F)) \cong F^+ \times F^+$
(iii) If $|F| = p^m$, then $UT(3,p^m) \in Syl_p(GL(3,p^m))$

Solution: (i) Let

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, \quad a,b,c,x,y,z \in F.$$

$$\text{Then} \quad AB = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix} \in UT(3,F)$$

$$A^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in UT(3,F).$$

Hence $UT(3,F)$ is a subgroup of $GL(3,F)$.

(ii) Now if

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in Z(UT(3,F)), \text{ then } AB = BA \text{ for all } B \in UT(3,F) \text{ implies}$$

$$A = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and every element of this type is contained in the center so

$$Z(UT(3,F)) = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid \quad b \in F \quad \}$$

Let

$$\begin{aligned} \varphi : F^+ &\longrightarrow \quad Z(UT(3,F)) \\ b &\longrightarrow \quad \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

φ is an isomorphism.

Now to see that $UT(3,F)/Z(UT(3,F)) \cong F^+ \times F^+$.
Let $\theta : UT(3,F)/Z(UT(3,F)) \longrightarrow F^+ \times F^+$.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} Z \longrightarrow (a,c)$$

θ is well defined and, moreover θ is an isomorphism.

(iii) Now all we need to do is to compare the order of $UT(3,p^m)$ and the order of the Sylow p-subgroup of $GL(3,p^m)$. It is easy to see that $|UT(3,p^m)| = p^{3m}$. And $|GL(3,p^m)| = (p^{3m}-1)(p^{3m}-p^m)(p^{3m}-p^{2m}) = p^{3m}((p^{3m}-1)(p^{2m}-1)(p^m-1))$. Hence p part are the same and we are done.

2.23. *Let $x \in G$, $D := \{x^g : g \in G\}$ and $U_i \leq G$ for i= 1,2. Suppose that $\langle D \rangle = G$ and $D \subseteq U_1 \cup U_2$. Then show that $U_1 = G$ or $U_2 = G$.*

Solution: Assume that $U_1 \neq G$. Then there exists $g \in G$ such that $x^g \notin U_1$ otherwise all conjugates of x is contained in U_1 and so $D \subseteq U_1$ which implies $U_1 = G$. Then $x^g \notin U_1$ implies $x^g \in U_2$ as $D \subseteq U_1 \cup U_2$. Now for any $u_1 \in U_1$, $(x^g)^{u_1} \notin U_1$ otherwise x^g will be in U_1 which is impossible. Then for any $u_1 \in U_1$ we obtain $(x^g)^{u_1} \in U_2$. Now U_2 is a subgroup and $x^g \in U_2$ so we have $(x^g)^{u_2} \in U_2$ for all $u_2 \in U_2$. As $\langle U_1 \cup U_2 \rangle = G$ we obtain $(x^g)^t \in U_2$ for all $t \in G$, i.e, $D \subseteq U_2$ this implies $\langle D \rangle \leq U_2$ but $\langle D \rangle = G \leq U_2$ which implies $U_2 = G$.

2.24. *Let $g_1, g_2 \in G$. Then show that $|g_1g_2| = |g_2g_1|$.*

Solution: We will show that if $|g_1g_2| = k < \infty$, then $|g_2g_1| = k$. Let $|g_1g_2| = k$. $\underbrace{(g_1g_2)(g_1g_2)....(g_1g_2)}_{k-times} = 1$. Then multiplying from left by g_1^{-1} and from right by g_2^{-1} we have $\underbrace{(g_2g_1)(g_2g_1)\dots(g_2g_1)}_{(k-1)-times} = {g_1}^{-1}{g_2}^{-1}$.
Now multiply from right first by g_2 and then g_1, we obtain
$\underbrace{(g_2g_1)(g_2g_1)...(g_2g_1)}_{k-times} = ((g_2g_1))^k = 1$. It cannot be less than k since we

may apply the above process and then reduce the order of (g_1g_2) less than k.

2.25. *Let $H \leq G$, $g_1, g_2 \in G$. Then $Hg_1 = Hg_2$ if and only if ${g_1}^{-1}H = {g_2}^{-1}H$.*

Solution: ($\Rightarrow$) If $Hg_1 = Hg_2$, then $H = Hg_2{g_1}^{-1}$ hence $g_2{g_1}^{-1} \in H$. Then H is a subgroup implies $(g_2{g_1}^{-1})^{-1} \in H$ i.e. $g_1{g_2}^{-1} \in H$. It follows that $g_1{g_2}^{-1}H = H$. Hence ${g_2}^{-1}H = {g_1}^{-1}H$.

($\Leftarrow$) If ${g_1}^{-1}H = {g_2}^{-1}H$, then $g_1{g_2}^{-1} \in H$ by the same idea in the first part we have $(g_1{g_2}^{-1})^{-1} \in H$, $g_2{g_1}^{-1} \in H$ i.e. $Hg_2{g_1}^{-1} = H$. This implies $Hg_1 = Hg_2$.

2.26. *Let $H \leq G$, $g \in G$ if $|g| = n$ and $g^m \in H$ where n and m are co-prime integers. Then show that $g \in H$.*

Solution: The integers m and n are co-prime so there exists $a, b \in \mathbb{Z}$ satisfying $an + bm = 1$. Then $g = g^{an+bm} = g^{an}g^{bm} = (g^n)^a(g^m)^b = g^{mb} \in H$. As H is a subgroup of G, $g^m \in H$ implies $g^{bm} \in H$ and $g^{na} = 1$. Hence $g^{mb} = g \in H$.

2.27. *Let $g \in G$ with $|g| = n_1n_2$ where n_1, n_2 co-prime positive integers. Then there are elements $g_1, g_2 \in G$ such that $g = g_1g_2 = g_2g_1$ and $|g_1| = n_1, |g_2| = n_2$.*

Solution: As n_1 and n_2 are relatively prime integers, there exist a and b in $\mathbb{Z}$ such that $an_1 + bn_2 = 1$. Observe that a and b are also relatively prime in $\mathbb{Z}$. Then $g = g^1 = g^{an_1+bn_2} = g^{an_1}g^{bn_2}$. Let $g_1 = g^{bn_2}$ and $g_2 = g^{an_1}$. Then $g_1^{n_1} = (g^{bn_2})^{n_1} = 1$, $g_2^{n_2} = (g^{an_1})^{n_2} = 1$ $g = g_1g_2 = g^{an_1+bn_2} = g^{bn_2+an_1} = g_2g_1$. Indeed $|g_1| = n_1$. If $g_1^m = 1$, then $m|n_1$ and $g_1^m = g^{bn_2m} = 1$. It follows that $n_1n_2|bn_2m$. Then $n_1|bm$ but by above observation n_1 and b are relatively prime as $an_1+bn_2 = 1$, so $n_1|m$. It follows that $n_1 = m$. Similarly $|g_2| = n_2$.

2.28. *Let g_1, $g_2 \in G$ with $|g_1| = n_1 < \infty, |g_2| = n_2 < \infty$, if n_1 and n_2 are co-prime and g_1 and g_2 commute, then $|g_1g_2| = n_1n_2$.*

Solution: The elements g_1 and g_2 commute. Therefore $(g_1g_2)^{n_1n_2} = g_1^{n_1n_2}g_2^{n_1n_2} = (g_1^{n_1})^{n_2}(g_2^{n_2})^{n_1} = 1$. Assume $|g_1g_2| = m$. Then $(g_1g_2)^m = g_1^mg_2^m = 1$. Then $m|n_1n_2$ and $g_1^m = g_2^{-m}$.
$(g_1^m)^{n_1} = (g_2^{-m})^{n_1} = 1$. Then $n_2|mn_1$ but $gcd(n_1, n_2) = 1$. We obtain

$n_2|m$. Similarly $n_1|m$ but $gcd(n_1, n_2) = 1$ implies $n_1n_2|m$. Hence $m = n_1n_2$.

2.29. *If $H \leq K \leq G$ and $N \lhd G$, show that the equations $HN = KN$ and $H \cap N = K \cap N$ imply that $H = K$.*

Solution: $HN \cap K = KN \cap K = K$. On the other hand by Dedekind law $HN \cap K = H(N \cap K) = H(N \cap H) = H$. Hence $H = K$.

2.30. *Given that $H_\lambda \lhd K_\lambda \leq G$ for all $\lambda \in \Lambda$, show that $\bigcap_\lambda H_\lambda \lhd \bigcap_\lambda K_\lambda$.*

Solution: Let $x \in \bigcap_\lambda H_\lambda$ and $g \in \bigcap_\lambda K_\lambda$. Then consider $g^{-1}xg$. Since, for any $\lambda \in \Lambda$, $g \in K_\lambda$ and $x \in H_\lambda$ and $H_\lambda \lhd K_\lambda$, we have $g^{-1}xg \in H_\lambda$ for all $\lambda \in \Lambda$. i.e $g^{-1}xg \in \bigcap_{\lambda \in \wedge} H_\lambda$.

2.31. *If a finite group G contains exactly one maximal subgroup, then G is cyclic.*

Solution: Let M be the unique maximal subgroup of G. Then every proper subgroup of G is contained in M. Since M is maximal there exists $a \in G \setminus M$. Then $\langle a \rangle = G$

2.32. *Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.*

Solution: Let $H = \{1, h\}$ be a subgroup of order 2. Clearly $C_G(H) \leq N_G(H)$. We need to show that if $|H| = 2$, then $N_G(H) \leq C_G(H)$. Let $g \in N_G(H)$. Then $g^{-1}hg$ is either 1 or h. If $g^{-1}hg = 1$, then $h = 1$ which is a contradiction. So $g^{-1}hg = h$ i.e $g \in C_G(H)$. So $C_G(H) = N_G(H)$. Moreover if $N_G(H) = G$ then $C_G(H) = N_G(H) = G$. This implies $H \leq Z(G)$.

2.33. *Let $\alpha \in AutG$. Suppose that $x^{-1}x^\alpha \in Z(G)$ for all $x \in G$. Then $x^\alpha = x$ for all $x \in G'$.*

Solution: Observe that $x^{-1}x^\alpha \in Z(G)$ implies that $x^\alpha x^{-1} \in Z(G)$ as $Z(G)$ is a subgroup and x is an arbitrary element in G. Take an arbitrary generator $a^{-1}b^{-1}ab \in G'$ where $a, b \in G$. Then

$$
\begin{aligned}
(a^{-1}b^{-1}ab)^{\alpha} &= (a^{-1})^{\alpha}(b^{-1})^{\alpha}(a)^{\alpha}(b)^{\alpha} \\
&= (a^{-1})^{\alpha}(b^{-1})^{\alpha}(a)^{\alpha}a^{-1}a(b)^{\alpha} \text{ as } a^{\alpha}a^{-1} \in Z(G) \\
&= (a^{-1})^{\alpha}(a)^{\alpha}a^{-1}(b^{-1})^{\alpha}a(b)^{\alpha} \\
&= a^{-1}(b^{-1})^{\alpha}a(b)^{\alpha} \\
&= a^{-1}b^{-1}\underbrace{b(b^{-1})^{\alpha}}a(b)^{\alpha} \\
&= a^{-1}b^{-1}a\underbrace{b(b^{-1})^{\alpha}}(b)^{\alpha} \\
&= a^{-1}b^{-1}ab
\end{aligned}
$$

For any generator $x \in G'$ we have $x^{\alpha} = x$. Hence for any $g \in G'$ we have $g^{\alpha} = g$

2.34. *Let $G = AA^g$ for some $g \in G$. Then $G = A$.*

Solution: It is enough to show that the specific element $g \in G$ is contained in A. For every element $x \in G$, there exist a_x, b_x in A such that $x = a_x b_x^g$. In particular $g = a_g b_g^g = a_g g^{-1} b_g g$. It follows that $a_g g^{-1} b_g = 1$ and $g^{-1} = a_g^{-1} b_g^{-1}$, then $g = b_g a_g \in A$ as a_g and b_g in A.

2.35. *Let G be a finite group and $A \leq G$ and $B \leq A$. If $x_1, x_2 \dots x_n$ is a transversal of A in G and $y_1, y_2 \dots y_m$ is a transversal of B in A, then $\{y_j x_i\}$, $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$ is a transversal of B in G.*

Solution: Let $G = \bigcup_{i=1}^{n} Ax_i$ and $Ax_i \cap Ax_j = \emptyset$ for all $i \neq j$ and $A = \bigcup_{i=1}^{m} By_i$ and $By_i \cap By_j = \emptyset$ for all $i \neq j$. Then we have,

$G = \bigcup_{i=1}^{n} Ax_i = \bigcup_{i=1}^{n} \left(\bigcup_{j=1}^{m} By_i\right) x_i = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} By_j x_i$

If $By_j x_i \cap By_r x_m \neq 0$, then $Ax_i \cap Ax_m \neq 0$ implying that $x_i = x_m$. Then $By_j x_i \cap By_r x_i \neq 0$. Hence $y_r = y_j$

2.36. *Suppose that $G \neq 1$ and $|G : M|$ is a prime number for every maximal subgroup M of G. Then show that G contains a normal maximal subgroup. (Maximal subgroups with the above properties exist by assumption).*

Solution: Let Σ be the set of all primes p_i such that $|G : M_i| = p_i$ where p_i is a prime.

So $\Sigma = \{p_i \ : \ |G : M_i| = p_i, M_i$ is a maximal subgroup of $G\}$. Let p be the smallest prime in Σ. Let M be a maximal subgroup of G such that $|G : M| = p$. Then G acts on the right to the set of right cosets of M in G. Let $\Omega = \{Mx \ : \ x \in G\}$. Then $|\Omega| = p$ and there exists a homomorphism

$$\phi : G \to Sym(\Omega)$$

such that $Ker\ \phi = \cap_{x\in G} M^x \leq M$. Then $G/Ker\ \phi$ is isomorphic to a subgroup of $Sym(\Omega)$ and $|Sym(\Omega)| = p!$. Then $G/Ker(\phi)$ is a finite group and there exists a maximal subgroup of G containing $Ker(\phi)$ and index of subgroup divides $p!$. But p was the smallest prime $|G : M| = p$ so this implies that $M = Ker\ (\phi)$ is a normal subgroup of G.

2.37. *If G acts transitively on Ω, then $N_G(G_\alpha)$ acts transitively on $C_\Omega(G_\alpha)$, $\alpha \in \Omega$.*

Solution $G_\alpha = \{g \in G |\ \alpha.g = \alpha \ \}$ and $C_\Omega(G_\alpha) = \{\beta \in \Omega \ | \ \beta.g = \beta$ for all $g \in G_\alpha \ \}$. Clearly $\alpha \in C_\Omega(G_\alpha)$. We will show that the orbit of $N_G(G_\alpha)$ containing α is $C_\Omega(G_\alpha)$.

Observe first that if $\beta \in C_\Omega(G_\alpha)$ and $x \in N_G(G_\alpha)$, then $\beta x \in C_\Omega(G_\alpha)$. Indeed for any $g_\alpha \in G_\alpha, \beta x.g_\alpha = \beta x g_\alpha x^{-1} x = \beta y x$ for some $y \in G_\alpha$. Hence $\beta x g_\alpha = \beta x$. i.e. $\beta x \in C_\Omega(G_\alpha)$. Let $\beta \in C_\Omega(G_\alpha)$. Since G is transitive on Ω, there exists $g \in G$ such that $\alpha.g = \beta$. Then for any $t \in G_\alpha$, $\alpha.gt = \alpha g$. i.e $gtg^{-1} \in G_\alpha$ for all $t \in G_\alpha$. i.e. $g \in N_G(G_\alpha)$. Therefore the orbit of $N_G(G_\alpha)$ containing α contains the set $C_\Omega(G_\alpha)$.

2.38. *Let G be a finite group.*
(a) *Suppose that $A \neq 1$ and $A \cap A^g = 1$ for all $g \in G \setminus A$.*
Then $|\bigcup_{g\in G} A^g| \geq \frac{|G|}{2} + 1$
(b) *If $A \neq G$, then $G \neq \bigcup_{g\in G} A^g$*

Solution: **(a)** If $A = G$, then the statement is already true. So assume that A is a proper subgroup of G. The number of distinct conjugates of A in G is the index $|G : N_G(A)| = k$.

Observe first that as$N_G(A) \geq A$ and $A \cap A^g = 1$ for all $g \in G \setminus A$ we have $N_G(A) = A$. Then $A^{g_i} \cap A^{g_j} = 1$ for all $i \neq j$ as $A^{g_i} \cap A^{g_j} \neq 1$ implies $A \cap A^{g_i g_j^{-1}} \neq 1$. It follows that $A = A^{g_i g_j^{-1}}$. This implies $A^{g_i} = A^{g_j}$ and we obtain $i = j$.

$|G : N_G(A)| = \frac{|G|}{|N_G(A)|} = \frac{|G|}{|A|} = k$. Then $|G| = k|A|$.

Now

$$\begin{aligned} |\bigcup_{g\in G} A^g| &= |\bigcup_{i=1}^{k} A^{g_i}| \\ &= k(|A|-1)+1 \\ &= k|A|-k+1 \\ &= |G|-k+1 \\ &\geq |G|-\frac{|G|}{2}+1 \text{ as } k \leq \frac{|G|}{2} \\ &= \frac{|G|}{2}+1 \end{aligned}$$

(b) By above if $A \neq G$, then $|\bigcup_{g\in G} A^g| = |G|-k+1$. Then $|G| = k-1+|\bigcup_{g\in G} A^g|$ as $k \geq 2$ we obtain $G \neq \bigcup_{g\in G} A^g$.

2.39. *If $H \leq G$, then $G \setminus H$ is finite if and only if G is finite or $H = G$.*

Solution: Assume that $H \leq G$ and $G \setminus H$ is finite. If $G \setminus H = \phi$ then, $G = H$. So assume that $G \setminus H \neq \phi$. If $x \in G \setminus H$, then the left coset xH has the same cardinality as H and $xH \cap H = \phi$, it follows that $xH \subseteq G \setminus H$. Hence H is finite. Similarly $\bigcup\limits_{t_i \neq 1} t_i H \subseteq G \setminus H$ finite where t_i belongs to the left transversal of H in G. But $G = \bigcup\limits_{t_i \neq 1} t_i H \cup H$. Union of two finite set is finite. Hence G is a finite group.

Converse is trivial.

2.40. *Let $d(G)$ be the smallest number of elements necessary to generate a finite group G. Prove that $|G| \geq 2^{d(G)}$*
(Note: *by convention $d(G) = 0$ if $|G| = 1$).*

Solution: By induction on $d(G)$. If $d(G) = 0$, then $|G| = 1$. The result is also true if $d(G) = 1$. Since the non-identity element has order at least 2. Hence $|G| \geq 2$. Let $d(G) = n$. Assume that if a group H is generated by $n-1$ elements, then $|H| \geq 2^{n-1}$.

Let the generators of G be $\{x_1, x_2, \cdots, x_n\}$. Then the subgroup $T = < x_1, x_2, \cdots, x_{n-1} >$ is a proper subgroup of G and by assumption

$|T| \geq 2^{n-1}$. Since $x_n \notin T$ we obtain x_nT is a left coset of T in G and $x_nT \cap T = \phi$. Moreover $x_nT \cup T \subseteq G$. Hence $|G| \geq |x_nT \cup T| = |x_nT| + |T| = 2|T| \geq 2\ 2^{n-1} = 2^n$.

2.41. *A group has exactly three subgroups if and only if it is cyclic of order p^2 for some prime p.*

Solution: Let G be a cyclic group of order p^2. Every finite cyclic group has a unique subgroup for any divisor of the order of G. Hence G has a unique subgroup H of order p. Hence H is the only nontrivial subgroup of G. Then the subgroups are $\{1\}$, H and G.

Conversely let G be a group which has exactly three subgroups. Since every group has $\{1\}$ and itself as trivial subgroups, G must have only one non-trivial subgroup, say H. So H has no nontrivial subgroups. This implies H is a cyclic group of order p for some prime p. Let $x \in G$. Then $x^{-1}Hx$ is again a subgroup of order p but G has only one subgroup of order p implies that $x^{-1}Hx = H$ for all $x \in G$ i.e. H is a normal subgroup of G. So we have the quotient group G/H. Since there is a $1-1$ correspondence between the subgroups of G/H and the subgroups of G containing H we obtain G/H has no nontrivial subgroup i.e. G/H is a group of order q for some prime q. Then $|G| = pq$ so G has a proper subgroup of order p and of order q. This implies

$$p = q \quad \text{and} \quad |G| = p^2.$$

Every group of order p^2 is abelian. Then either G is cyclic of order p^2 or $G \cong Z_p \times Z_p$. But if G is isomorphic to $Z_p \times Z_p$ then G has 5 subgroups but this is impossible as we have only three subgroups. Hence G is a cyclic group of order p^2.

Another Solution: Let G be a group with exactly 3 subgroups. Since $\{1\}$ and $\{G\}$ are subgroups of G we have only one nontrivial proper subgroup H of G. Since H has no nontrivial subgroup. It is a group of order p for some prime p, say $H = \langle x \rangle$, since $G \neq H$ there exists $y \in G \setminus H$. Then $\langle y \rangle$ is a subgroup of G different from H. Hence $\langle y \rangle = G$. So G is a cyclic group, and has a subgroup H of order p. This implies G is a finite cyclic group. Since for any divisor of the order of a cyclic group, there exists a subgroup, the only prime divisor of $|G|$

must be p. And $|G|$ must be p^2 otherwise G has a subgroup for the other divisors.

2.42. *Let H and K be subgroups of a finite group G.*

(a) Show that the number of right cosets of H in HdK equals $|K : H^d \cap K|$

(b) Prove that

$$\sum_d \frac{1}{|H^d \cap K|} = \frac{|G|}{|H|\,|K|} = \sum_d \frac{1}{|H \cap K^d|}$$

where d runs over a set of (H,K)-double coset representatives.

Solution: **(a)** The function $\alpha : HdK \to HdKd^{-1}$
$hdk \to hdkd^{-1}$
is a bijective function. Hence $|HdK| = |HdKd^{-1}| = |H \cdot K^d|$. Similarly $\beta : HdK \to d^{-1}HdK$ is bijective. Hence

$$|HdK| = |HK^d| = |d^{-1}HdK| = |H^dK|$$

Since H and K^d are subgroups of G we have $|HdK| = |HK^d|$.

$$|HdK| = |HK^d| = \frac{|H|\,|K^d|}{|H \cap K^d|} = \frac{|H|\,|K|}{|H \cap K^d|}$$

$$\frac{|HdK|}{|H|} = \frac{|H^dK|}{|H|} = \frac{|H^d|\,|K|}{|H|\,|H^d \cap K|} = \frac{|K|}{|H^d \cap K|}$$

$$= |K : K \cap H^d|$$

(b)

$$\frac{|G|}{|H|\,|K|} = \sum_d \frac{|HdK|}{|H|\,|K|} = \sum_d \frac{|K|}{|H^d \cap K|\,|K|} = \sum_d \frac{1}{|H^d \cap K|}$$

similarly

$$\frac{|G|}{|H|\,|K|} = \sum_d \frac{|HdK|}{|H|\,|K|} = \sum_d \frac{|H|\,|K^d|}{|H \cap K^d| \cdot |H|\,|K|} = \sum_d \frac{1}{|H \cap K^d|}$$

2.43. *Find some non-isomorphic groups that are direct limits of cyclic groups of order $p, p^2, p^3, \cdots$.*

Solution: Let the finite cyclic group G_i of order p^i be generated by x_i. Recall that a cyclic group has a unique subgroup for any divisor of the order of the group.

$$\alpha_i^{i+1} : \begin{array}{c} G_i \hookrightarrow G_{i+1} \\ x_i \hookrightarrow x_{i+1}^p \end{array}$$

The homomorphisms α_i^{i+1} is a monomorphism. So direct limit is the locally cyclic (quasi-cyclic or Prüfer) group denoted by C_{p^∞}.

(b) $\alpha_i^{i+1} : \begin{array}{c} G_i \hookrightarrow G_{i+1} \\ x_i \hookrightarrow 1 \end{array}$. Then $D = \lim_{n\to\infty} G_n = \{1\}$.

2.44. *If $H \leq G$, prove that $H^G = \langle H^g | \; g \in G\rangle$ and $H_G = \bigcap_{g\in G} H^g$.*

Solution: Recall that H^G is the intersection of all normal subgroups containing H. Let $M = \langle H^g | \; g \in G\rangle$ we need to show that $M = H^G$. Every element $x \in M$ is of the form $x = h_1^{g_1} h_2^{g_2} \cdots h_k^{g_k}$. Then for any element

$$g \in G, \quad x^g = (h_1^{g_1} \cdots h_k^{g_k})^g = h_1^{g_1 g} h_2^{g_2 g} \cdots h_k^{g_k g} \in M.$$

Hence M is a normal subgroup of G. If we choose $g = 1$ in h^g we obtain $H \leq M$. Hence M is a normal subgroup containing H i.e. $M \supseteq H^G$. On the other hand H^G is a normal subgroup of G containing H. Hence H^G contains all elements of the form h^g, $g \in G$. In particular $H^G \supseteq M$. Hence $M = H^G$.

H_G is the join of normal subgroups of G contained in H. Recall that H_G is the largest normal subgroup, contained in H.

For the second part, let, $T = \bigcap_{g\in G} H^g$.

If we choose $g = 1$ we obtain $H^g = H$. Hence $T \subseteq H$. Intersection of subgroups is a subgroup, hence T is a subgroup of G.

Let $x \in T$. Then $x \in H^y$ for all $y \in G$. It follows that $x^g \in H^{yg}$ for all $y \in G$. But $\bigcap\limits_{y\in G} H^y = \bigcap\limits_{y\in G} H^{yg}$ since the function $\alpha_g : \begin{array}{c} G \to G \\ y \to yg \end{array}$ is $1-1$ and onto. Hence T is a normal subgroup of G contained in H. It follows that $T \subseteq H_G$.

On the other hand H_G is a normal subgroup of G contained in H. Then $H_G^g \leq H^g$ for all $g \in G$. But $H_G^g = H_G$ implies $H_G \leq \bigcap\limits_{g\in G} H^g = T$.

Hence $T = H_G$.

2.45. *If H is abelian, then the set of homomorphisms Hom (G, H) from G into H is an abelian group, if the group operation is defined by $g^{\alpha+\beta} = g^\alpha g^\beta$.*

Solution: Let $\alpha, \beta, \gamma \in$ Hom (G, H). Then for any $g \in G$

$$\begin{aligned} g^{\alpha+(\beta+\gamma)} &= g^\alpha \, g^{\beta+\gamma} = g^\alpha (g^\beta g^\gamma). \\ &= (g^\alpha g^\beta) g^\gamma \\ &= g^{\alpha+\beta} \cdot g^\gamma = g^{(\alpha+\beta)+\gamma} \end{aligned}$$

By associativity in H.

Hence $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

The zero homomorphism, namely the map which takes every element g in G to the identity element in H.

For any $\alpha \in$ Hom (G, H)

$$g^{-\alpha} = (g^{-1})^\alpha$$

$$g^{\alpha-\alpha} = g^\circ = 1$$

Hence $-\alpha$ is the inverse of α.

$$\begin{aligned} g^{\alpha+\beta} &= g^\alpha g^\beta = g^\beta g^\alpha \quad \text{since} \quad H \quad \text{is abelian} \\ &= g^{\beta+\alpha}. \quad \text{Hence} \quad \alpha + \beta = \beta + \alpha \end{aligned}$$

for all $\alpha, \beta \in$ Hom (G, H) $g^{\alpha+\beta} = g^\alpha g^\beta$, then $\alpha+\beta$ is a homomorphism.

$$\begin{aligned} (gh)^{\alpha+\beta} = (gh)^\alpha (gh)^\beta &= g^\alpha h^\alpha \, g^\beta h^\beta \\ &= g^\alpha g^\beta \cdot h^\alpha h^\beta \quad \text{since} \quad H \quad \text{is abelian.} \\ &= g^{\alpha+\beta} h^{\alpha+\beta} \end{aligned}$$

Observe that commutativity of H is used in order to have $\alpha + \beta \in$ Hom (G, H).

2.46. *If G is n-generator and H is finite, prove that*

$$|Hom(G, H)| \leq |H|^n.$$

Solution: Let G be generated by $g_1, g_2, \cdots, g_n$ and α be a homomorphism. α is uniquely determined by the n tuple $g_1^\alpha, g_2^\alpha, \cdots, g_n^\alpha$. For this if β is another homomorphism from G into H, such that $g_i^\alpha = g_i^\beta$. Then for any element $g \in G$

$$g = g_{i_1}^{n_{i1}} g_{i_2}^{n_{i2}} \cdots g_{i_k}^{n_{ik}}$$

where $g_{i_j} \in \{g_1, \cdots, g_n\}$ for all $i_j \in \{1, 2, \cdots, n\}$ and $n_{i_j} \in Z$. Since α and β are homomorphisms from G into H.

$$\begin{aligned} g^{\alpha} &= \left(g_{i_1}^{n_{i_1}} \right)^{\alpha} \left(g_{i_2}^{n_{i_2}} \right)^{\alpha} \cdots \left(g_{i_k}^{n_{ik}} \right)^{\alpha} \\ g^{\beta} &= \left(g_{i_1}^{n_{i_1}} \right)^{\beta} \left(g_{i_2}^{n_{i_2}} \right)^{\beta} \cdots \left(g_{i_k}^{n_{i_k}} \right)^{\beta} \end{aligned}$$

It follows that for any $g \in G$, $g^{\alpha} = g^{\beta}$. Hence $\alpha = \beta$. H is finite and there are at most $|H|^n$, n-tuple. Hence the number of homomorphisms from G into H is less than or equal to $|H|^n$.

2.47. *Show that the group $T = \{\frac{m}{2^n} \; | m, n \in \mathbb{Z}\}$ is a direct limit of infinite cyclic groups.*

Solution Let G_i be an infinite cyclic group generated by x_i. Define a homomorphism $\alpha_i^{i+1} : \begin{array}{l} G_i \hookrightarrow G_{i+1} \\ x_i \hookrightarrow x_{i+1}^2 \end{array}$

$$\alpha_i^j = \alpha_i^{i+1} \alpha_{i+1}^{i+2} \cdots \alpha_{j-1}^j$$

and

$$\alpha_i^j : \begin{array}{l} G_i \to G_j \\ x_i \to x_j^{2^{j-i}} \end{array}$$

Then the set $\sum = \left\{ (G_i, \alpha_i^j) : \quad i \leq j \right\}$ is a direct system.

Let D be the direct limit of the above direct system. Then

$$\begin{aligned} \overline{G}_1 &= \{[x_1^j] \mid \quad j \in \mathbb{Z}\} \leq D \\ \overline{G}_2 &= \{[x_2^j] \mid \quad j \in \mathbb{Z}\} \leq D \end{aligned}$$

$\overline{G}_1 \leq \overline{G}_2$. Because

$$[x_1^j] = [(x_1)^j \alpha_1^2] = [x_2^{2j}] \in \overline{G}_2$$

Let $D = \displaystyle\bigcup_{i=1}^{\infty} \overline{G}_i$. Then D is an abelian group. Indeed assume that $i \leq j$. $[x_i^n][x_j^m] = [x_i^n(\alpha_i^j) x_j^m] = [x_j^{n2^{j-i}} \cdot x_j^m] = [x_j^m \cdot x_j^{n2^{j-i}}] = [x_j^m][x_j^{n2^{j-i}}] = [x_j^m][x_i^n]$.

Claim: $D \cong T = \{\frac{n}{2^i} | \; n, i \in \mathbb{Z}\} \leq (\mathbb{Q}, +)$

$$\varphi : D \to T$$

$$[x_i^k] \to \frac{k}{2^i}$$

Let $[x_i^n]$ and $[x_j^m]$ be elements of D. Assume that $i \leq j$. Then $[x_i^n][x_j^m] = [x_j^{n2^{j-i}+m}]$

$$[x_i^n] \xrightarrow{\varphi} \frac{n}{2^i}$$

$$[x_j^m] \xrightarrow{\varphi} \frac{m}{2^j}$$

$$[x_i^n][x_j^m] = [x_j^{n2^{j-i}+m}] \xrightarrow{\varphi} \frac{n2^{j-i}+m}{2^j}$$

Now

$$\frac{n}{2^i} + \frac{m}{2^j} = \frac{n \cdot 2^{j-i}}{2^j} + \frac{m}{2^j} = \frac{n2^{j-i}+m}{2^j}.$$

So φ is a homomorphism from D into T. Clearly φ is onto.

$$\text{Ker } \varphi = \{\ [x_i^m] \mid \ \varphi[x_i^m] = \frac{m}{2^i} = 0\} = \{[x_i^\circ]\} = \{[1]\} \in D$$

so φ is an isomorphism.

2.48. *Show that* $\mathbb{Q}$ *is a direct limit of infinite cyclic groups.*

Solution: Recall that for any two infinite cyclic groups generated by x and y the map

$$\begin{aligned} \langle x \rangle > \to \ \langle y \rangle \\ x \to y^m \end{aligned}$$

for any m defines a homomorphism. Moreover this map is a monomorphism. Observe that the set of natural numbers $\mathbb{N}$ is a directed set with respect to natural ordering. Let G_i be an infinite cyclic group generated by $x_i, i = 1, 2, 3, \cdots$

Define a homomorphism $\alpha_i^{i+1} : \begin{array}{l} G_i \hookrightarrow G_{i+1} \\ x_i \hookrightarrow x_{i+1}^{i+1} \end{array}$

where α_i^i is identity.

$$\alpha_i^{i+1}\alpha_{i+1}^{i+2} = \alpha_i^{i+2} : \qquad x_i \to x_{i+1}^{i+1} \to (x_{i+2})^{(i+2)(i+1)}$$

$$\alpha_i^j = \alpha_i^{i+1}\alpha_{i+1}^{i+2} \cdots \alpha_{j-1}^j$$

The set $\left\{(G_i, \alpha_i^j)|\ \ i \le j\right\}$ is a direct system. The equivalence class of x_1 contains the following set

$$\begin{aligned}
[x_1] &= \{x_1, x_2^2, x_3^6, x_4^{24}, x_5^{5!}, \cdots, x_n^{n!}, \cdots\} \\
[x_2] &= \{x_2, x_3^3, x_4^{12}, x_5^{5\cdot 4\cdot 3}, \cdots, x_k^{k\cdot(k-1)\cdots 3}, \cdots\} \\
[x_3] &= \{x_3, x_4^4, x_5^{20}, x_6^{6\cdot 5\cdot 4}, \quad , x_k^{k\cdot(k-1)(k-2)\cdots 4}, \cdots\} \\
&\vdots \\
[x_{n-1}] &= \{x_{n-1}, x_n^n, x_{n+1}^{(n+1)n}, \cdots\} \\
[x_n] &= \{x_n, x_{n+1}^{n+1}, x_{n+2}^{n+2\cdot n+1}, \cdots, x_k^{k\cdot(k-1)\cdots(n+1)}, \cdots\}
\end{aligned}$$

$$\begin{aligned}
[x_2]^2 &= [x_2][x_2] = [x_1] \\
[x_3]^3 &= [x_3][x_3][x_3] = [x_2] \\
[x_4]^4 &= [x_4][x_4][x_4][x_4] = [x_3] \\
&\vdots
\end{aligned}$$

$$[x_n]^n = [x_n]\cdots[x_n] = [x_n^n] = [x_{n-1}]$$

$$[x_n]^{n!} = [x_1]$$

since $G_i = \langle x_i \rangle$, the direct limit $D = \lim_{n\to\infty} G_i = \langle [x_i]\ |i = 1, 2, 3, \cdots\rangle$

Define a map

$$\varphi : \begin{array}{l} \varphi : D \to (\mathbb{Q}, +) \\ [x_n] \to \frac{1}{n!} \end{array}$$

if $m > n$

$$\begin{aligned}
[x_n][x_m] &= [x_n^{\alpha_n^m}][x_m] \\
&= [x_m^{(n+1)(n+2)\cdots m}][x_m] \\
&= [x_m^{(n+1)(n+2)\cdots m+1}] \\
[x_n][x_m] &= [x_m^{(n+1)(n+2)\cdots m+1}]
\end{aligned}$$

$$x_n \to \tfrac{1}{n!}$$
$$x_m \to \tfrac{1}{m!}$$
$$x_m^{(n+1)(n+2)\cdots m+1} \to \frac{(n+1)(n+2)\cdots m+1}{m!}$$

For $m \ge n$.

$$\frac{1}{n!} + \frac{1}{m!} = \frac{(n+1)(n+2)\cdots m}{m!} + \frac{1}{m!} = \frac{(n+1)\cdots(m)+1}{m!}$$

so φ is a homomorphism. For any $\dfrac{m}{n} \in \mathbb{Q}$ we have $\varphi([x_n]^{(n-1)!m}) = \frac{1}{n!}^{(n-1)!m} = \frac{m}{n}$. Hence φ is onto

$$\text{Ker } \varphi = \left\{ [x_{i_1}]^{k_1} [x_{i_2}]^{k_2} \cdots [x_{i_j}]^{k_j} \in D \;\mid\; \varphi([x_i]^{k_1} \cdots [x_{ij}]^{kj}) = 1 \right\}$$

Since the index set is linearly ordered this corresponds to, there exists $n \in \mathbb{N}$ such that $n = \max\{i_1, \cdots, i_j\}$. Hence $[x_{i1}]^{k_1} \cdots [x_{i_j}]^{k_j} = [x_n]^m$ for some m. Then $\varphi[[x_n]^m] = \frac{m}{n!} = 0$. It follows that $m = 0$.

Then $[x_n]^0 = [x_1]^0 = [x_1^0]$ which is the identity element in D. Hence φ is an isomorphism.

Remark: On the other hand observe that $\varphi([x_n]^m) = \frac{m}{n!} = 1$ implies $m = n!$. Then $[x_n]^{n!} = [x_1]$ and $\varphi([x_1]) = \dfrac{1}{1!} = 1$.

2.49. *If G and H are groups with coprime finite orders, then Hom (G, H) contains only the zero homomorphism.*

Solution: Let α in Hom (G, H). Then by first isomorphism theorem $G/\text{Ker}\alpha \cong Im(\alpha)$.

By Lagrange theorem $|\text{Ker}(\alpha)|$ divides the order of $|G|$. Hence $\frac{|G|}{|\text{Ker}(\alpha)|}$ is coprime with $|H|$. Similarly $Im(\alpha) \leq H$ and $|Im(\alpha)|$ divides the order of H. Hence $\frac{|G|}{|\text{Ker}(\alpha)|} = |Im(\alpha)| = 1$. Hence $|\text{Ker}(\alpha)| = |G|$. This implies that α is a zero homomorphism i.e. α sends every element $g \in G$ to the identity element of H.

2.50. *If an automorphism fixes more than half of the elements of a finite group, then it is the identity automorphism.*

Solution Let α be an automorphism of G which fixes more than half of the elements of G. Consider the set $H = \{g \in G \mid g^\alpha = g\}$ We show that H is a subgroup of G. Indeed if $g_1, g_2 \in H$ then $g_1^\alpha = g_1$, $g_2^\alpha = g_2$. Hence $(g_1g_2)^\alpha = g_1^\alpha g_2^\alpha = g_1g_2$ i.e. $g_1g_2 \in H$. Moreover $(g_1^{-1})^\alpha = (g_1^\alpha)^{-1} = g_1^{-1}$. Hence $g_1^{-1} \in H$. So H is a subgroup of G containing more than half of the elements of G. By Lagrange theorem $|H|$ divides $|G|$. It follows that $H = G$.

2.51. *Let G be a group of order $2m$ where m is odd. Prove that G contains a normal subgroup of order m.*

Solution Let ρ be a right regular permutation representation of G . By Cauchy's theorem there exists an element $g \in G$ such that $|\langle g \rangle| = 2$. We write g as a permutation $g^\rho = (x_1, x_1 g^\rho)(x_2, x_2 g^\rho) \dots (x_m, x_m g^\rho)$. Since G^ρ is a regular permutation group it does not fix any point . It follows that any orbit of g^ρ containing a point x is of the form $\{x, xg^\rho\}$. Hence we have m transpositions. Since m is odd g^ρ is an odd permutation. Then the map

$$Sign : G^\rho \to \{1, -1\}$$

is onto. Hence $Ker(Sign) \lhd G^\rho$ and $|G/Ker(Sign)| = 2$. It follows that $|Ker(Sign)| = m$.

2.52. *Let G be a finite group and $x \in G$. Then $|C_G(x)| \geq |G/G'|$ where G' denotes the derived subgroup of G.*

Solution G acts on G by conjugation. Then stabilizer of a point is $C_G(x)$. Hence $|G : C_G(x)| = |\{x^g \mid g \in G\}|=$ length of the orbit containing x. It follows that $\frac{|G|}{|C_G(x)|} = |\{g^{-1}xg \mid g \in G\}|$. The function

$$\phi : \{g^{-1}xg \mid g \in G\} \to \{x^{-1}g^{-1}xg \mid g \in G\}$$

is a bijective function. But G' is generated by the elements $y^{-1}g^{-1}yg = [y, g]$ where y and g lies in G. It follows that

$$|\{x^{-1}g^{-1}xg \mid g \in G\} \leq |\{y^{-1}g^{-1}yg \mid y, g \in G\}| \leq |G'|.$$

Hence $\frac{|G|}{|C_G(x)|} \leq |G'|$. Then $|G/G'| \leq |C_G(x)|$.

2.53. *If H, K, L are normal subgroups of a group, then $[HK, L] = [H, L][K, L]$.*

Solution The group $[H, L]$ is generated by the commutators $[h, l] = h^{-1}l^{-1}hl$ where $h \in H$ and $l \in L$. Of course every generator $[h, l]$ of $[H, L]$ is contained in $[HK, L]$. Hence $[H, L]$ is a subgroup of $[HK, L]$. Similarly $[K, L]$ is contained in $[HK, L]$ hence $[H, L][K, L] \subseteq [HK, L]$. On the other hand generators of $[HK, L]$ are of the form $[hk, l] = [h, l]^k[k, l]$ where $h \in H$ and $l \in L$. The right hand side is an element of $[H, L][K, L]$ since H, K, L are normal subgroups, hence $[H, L]$ is normal in G and so $[h, l]^k \in [H, L]$. It follows that $[HK, L] \leq [H, L][K, L]$. Then we have the equality $[HK, L] = [H, L][K, L]$.

2.54. *Let α be an automorphism of a finite group G. Let*

$$S = \{g \in G \mid g^{\alpha} = g^{-1} \}.$$

If $|S| > \frac{3}{4}|G|$, show that α inverts all the elements of G and so G is abelian.

Solution Let $x \in S$. Then $|S \cup xS| = |S| + |xS| - |S \cap xS|$. Since $S \cup xS \subseteq G$, we obtain $|S \cup xS| \leq |G|$. On the other hand the function

$$\phi_x : \begin{array}{l} S \to xS \\ s \to xs \end{array}$$

is a bijective function. Hence $|xS| = |S|$. It follows that $|G| \geq |S \cup xS| = |S| + |S| - |S \cap xS|$. Then $|G| > \frac{3}{4}|G| + \frac{3}{4}|G| - |S \cap xS|$. It follows that $|S \cap xS| > \frac{3}{2}|G| - |G| = \frac{1}{2}|G|$. This is true for all $x \in S$. Let xs_1 and xs_2 be two elements of $S \cap xS$, then $xs_i \in S$ implies $(xs_i)^{\alpha} = x^{\alpha}s_i^{\alpha} = (xs_i)^{-1} = s_i^{-1}x^{-1} = x^{\alpha}s_i^{\alpha} = x^{-1}s_i^{-1}$. It follows that x and s_i commute. Since there are more than $\frac{1}{2}|G|$ elements in $|S \cap xS|$ we obtain $|C_G(x)| > \frac{1}{2}|G|$. But $C_G(x)$ is a subgroup. Hence by Lagrange theorem we obtain $|C_G(x)| = |G|$ which implies $G = C_G(x)$ i.e $x \in Z(G)$. But this is true for all $x \in S$. Hence $S \subseteq Z(G)$. So $\frac{3}{4}|G| < |S| \leq |Z(G)|$ and $Z(G)$ is a subgroup of G implies that $Z(G) = G$. Hence G is abelian. Then S becomes a subgroup of G. Hence S is a subgroup of G of order greater than $\frac{3}{4}|G|$. It follows by Lagrange theorem that $S = G$.

2.55. *Show that no group can have its automorphism group cyclic of odd order greater than* 1.

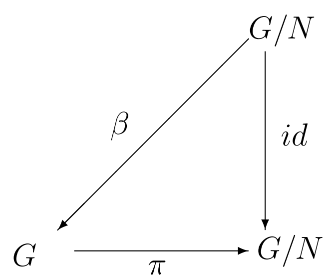
Solution Recall that if an element of order 2 in G exists, then by Lagrange theorem 2 must divide the order of the group.

We first show that the group in the statement of the question can not be an abelian group. If G is abelian, then the automorphism $x \to x^{-1}$ is an automorphism of G of order 2 unless $x = x^{-1}$ for all $x \in G$. By assumption the automorphism group is cyclic of odd order so $x = x^{-1}$ for all $x \in G$. It follows that G is an elementary abelian 2-group. Then G can be written as a direct sum of cyclic groups of order 2. This allows us to view G as a vector space over the field $\mathbb{Z}_2$. Then $Aut(G) \cong GL(n, \mathbb{Z}_2)$. As $|GL(2, \mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 3.2 = 6$.

The group $Aut(G) \cong GL(2, \mathbb{Z}_2)$ is cyclic of odd order. This group is cyclic if and only if $n = 1$ in that case $G \cong \mathbb{Z}_2$ and $Aut(G) = 1$ which is impossible by the assumption. So we may assume that G is non-abelian. Then there exists $x \in G \setminus Z(G)$. The element x induces a nontrivial inner automorphism of G. Moreover $G/Z(G) \cong Inn(G) \leq Aut(G)$. So $G/Z(G)$ is a cyclic group But this implies G is abelian. This is a contradiction. Hence such an automorphism does not exist.

2.56. *If $N \lhd G$ and G/N is free, prove that there is a subgroup H such that $G = HN$ and $H \cap N = 1$. (Use projective property).*

Solution Let π be the projection from G into G/N. Then by the projective property of the free group the diagram



commutes.

Since β is a homomorphism, $Im(\beta)$ is a subgroup of G. Let $H = Im(\beta)$. Let $w \in H \cap N$. Since $w \in N$, $wN = N$. The map β is a homomorphism implies $(wN)\beta = (N)\beta = id_G$ so $w = id$.

Let g be an arbitrary element of G. Now $gN \in G/N$ and $(gN)\beta \in H$, since the diagram is commutative $(gN)\beta\pi = gN$. By the projection π we have $(gN)\beta = gn$ for some $n \in N$. Hence $g = (gN)\beta.n^{-1}$ where $(gN)\beta \in H$ and $n^{-1} \in N$ i.e. $G = HN$.

2.57. *Prove that free groups are torsion free.*

Solution Let F be a free group on a set X. We may consider the elements of F as in the normal form. i.e. every element w in F can be written uniquely in the form $w = x_1^{l_1} \dots x_k^{l_k}$ where $x_i \in X$ and $l_i \in \mathbb{Z}$ for all $i = 1, 2, \dots, k$ and $x_i \neq x_j$ for $i \neq j$. Observe first that the elements x_i or x_i^{-1} have infinite orders.

Let $w = x_1^{l_1} \dots x_k^{l_k}$ be an arbitrary non-identity element of F. $w^2 = x_1^{l_1} \dots x_k^{l_k} x_1^{l_1} \dots x_k^{l_k}$. If $x_1^{l_1} \neq x_k^{-l_k}$, then for any n, w^n is nonidentity and we are done. If $x_1^{l_1} = x_k^{-l_k}$, then in w^2 these two elements cancel and gives identity. But it may happen that $x_2^{l_2} = x_{k-1}^{-l_{k-1}}$. Then the element w is of the form $x_1^{l_1}x_2^{l_2}\dots x_2^{-l_2}x_1^{-l_1}$. Then continuing like this we reach to an element $x_1^{l_1}x_2^{l_2}\dots x_i^{l_i}x_i^{-l_i}\dots x_2^{-l_2}x_1^{-l_1}$. But this implies that w is identity. So there exists i such that when we take powers of w then the powers of x_i increase. Since x_i has infinite order we obtain, w has infinite order.

2.58. *Prove that a free group of rank greater than one has trivial center.*

Let $w = x_1^{l_1}\dots x_n^{l_n}$ be an element of a center of a free group of rank > 1. If $x_1 \neq x_n$. Then $x_1^{l_1}\dots x_n^{l_n}x_1 \neq x_1x_1^{l_1}\dots x_n^{l_n}$. Since every element of F can be written uniquely and any two elements are equal if the corresponding entries are equal.

If $x_1 = x_n$, then consider wx_2x_1. By uniqueness of writing $wx_2x_1 \neq x_2x_1w$. This also shows that even if w contains only one symbol if rank of F is greater than one, then center of F is identity.

2.59. *Let F be a free group and suppose that H is a subgroup with finite index. Prove that every nontrivial subgroup of F intersects H nontrivially.*

Solution The group H has finite index in F implies that F acts on the right to the set $\Omega = \{Hx_1, \dots, Hx_n\}$ of the right cosets of H in F. Then there exists a homomorphism $\phi : F \to Sym(\Omega)$ such that $Ker\phi = \bigcap_{i=1}^{n} H^{x_i}$. Hence $F/Ker(\phi)$ is a finite group. Let K be a nontrivial subgroup of F and let $1 \neq w \in K$. Then $w^{n!} \neq 1$ since every nontrivial element of F has infinite order by 2.57. But $w^{n!} \in Ker\phi \leq H$. Hence $1 \neq w^{n!} \in K \cap Ker(\phi)$.

2.60. *If M and N are nontrivial normal nilpotent subgroups of a group. Prove from first principals that $Z(MN) \neq 1$. Hence give an* *alternative proof of Fittings Theorem for finite groups.*

Solution Consider $M \cap N$. If $M \cap N = 1$, then $MN = M \times N$ and $Z(MN) = Z(M) \times Z(N) \neq 1$. As M and N are nilpotent. If $M \cap N \neq 1$, then $[[M \cap N, M], M] \ldots] = 1$ implies there exists a subgroup $K \lhd (M \cap N)$ such that $1 \neq K \leq Z(M)$. Since $K \lhd N$ we have $[[K, N], N \ldots] = 1$. It follows that there exists a subgroup $1 \neq L \leq K$ such that $L \leq Z(N)$. Hence we obtain $1 \neq L \leq Z(M) \cap Z(N)$. But $1 \neq L \leq Z(M) \cap Z(N) \leq Z(MN)$.

Let $Z = Z(MN) Char MN \lhd G$ implies $Z \lhd G$. Hence MZ/Z and NZ/Z are normal nilpotent subgroups of G/Z. Then MN/Z has a nontrivial center in G/Z. Continuing like this if MN is finite we obtain a central series of MN. Hence MN is a nilpotent group in the case that MN is a finite group.

2.61. *Let A be a nontrivial abelian group and set $D = A \times A$. Define $\delta \in Aut(D)$ as follows: $(a_1, a_2)^\delta = (a_1, a_1 a_2)$. Let G be the semidirect product $\langle \delta \rangle \ltimes D$.*

(a) *Prove that G is nilpotent of class 2 and $Z(G) = G' \cong A$*

(b) *Prove that G is a torsion group if and only if A has finite exponent.*

(c) *Deduce that even if the center of a nilpotent group is a torsion group, the group may contain elements of infinite order.*

Solution Let A be a nontrivial abelian group. Define δ on $D = A \times A$ such that $\delta(a_1, a_2) = (a_1, a_1 a_2)$. Then δ is an automorphism of D. Indeed $\delta((a_1, a_2)(b_1, b_2)) = \delta(a_1 b_1, a_2 b_2) = (a_1 b_1, a_1 b_1 a_2 b_2) = (a_1, a_1 a_2)(b_1, b_1 b_2)$ as A is an abelian group. So δ is a homomorphism from D into D.

$$Ker(\delta) = \{(a_1, a_2) | \quad \delta(a_1, a_2) = (a_1, a_1 a_2) = (1, 1)\} = \{(1, 1)\}$$

Moreover for any $(a_1, a_2) \in D$, $\delta(a_1, a_1^{-1} a_2) = (a_1, a_2)$. Hence δ is an automorphism of D. Therefore we may form the group G as a semidirect product of D and $\langle \delta \rangle$ and obtain $G = D \rtimes \langle \delta \rangle$

(a) Now we show that $Z(G) = G' \cong A$.

An element of G is of the form $(\delta^i,(a_1,a_2))$ for some $i\in\mathbb{Z}$ and a_1,a_2 in A. Let $(\delta^n,(z_1,z_2))$ be an element of the center of G. Then

$(\delta^i,(a_1,a_2))^{-1}(\delta^n,(z_1,z_2))(\delta^i,(a_1,a_2) = (\delta^n,(z_1,z_2))$ for any $i\in\mathbb{Z}$ and for any $(a_1,a_2)\in A\times A$.

Then

$(\delta^i,(a_1,a_2))^{-1}(\delta^{n+i},(z_1,z_2)^{\delta^i}(a_1,a_2)) = (\delta^i,(a_1,a_2))^{-1}(\delta^{n+i},(z_1,z_1^i z_2)(a_1,a_2))$
$= (\delta^i,(a_1,a_2))^{-1}(\delta^{n+i},(z_1a_1,z_1^iz_2a_2)$.

Observe that $(\delta^i,(a_1,a_2))^{-1} = (\delta^{-i},(a_1^{-1},a_1^ia_2^{-1}))$,
we obtain $(\delta^{-i},(a_1^{-1},a_1^ia_2^{-1}))(\delta^{n+i},(z_1a_1,z_1^iz_2a_2)$

$$= (\delta^n,(a_1^{-1},a_1^ia_2^{-1})^{\delta^{n+i}}(z_1a_1,z_1^iz_2a_2)$$
$$= (\delta^n,(a_1^{-1},a_1^{-n}a_2^{-1}(z_1a_1,z_1^iz_2a_2))$$
$$= (\delta^n,(a_1^{-1},(a_1^{-1})^na_2^{-1})(z_1a_1,z_1^iz_2a_2))$$
$$= (\delta^n,(z_1,a_1^{-n}z_1^iz_2)$$
$$= (\delta^n,(z_1,z_2))$$

implies that $a_1^{-n}z_1^i = 1$. So $z_1^i = a_1^n$ for any i and for any $a_1\in A$. In particular $a_1 = 1$ implies that $z_1 = 1$. It follows that $a_1^n = 1$ for any $a_1\in A$. Then $(a_1,a_2)^{\delta^n} = (a_1,a_1^na_2) = (a_1,a_2)$.

Hence δ^n is an identity automorphism of D. It follows that $(\delta^n,(1,z_2)) = (id,(1,z_2))$.

Hence $Z(G) = \{(1,(1,z)) : \quad z\in A\ \}\cong A$.

The group G' is generated by commutators. The form of a general commutator is:

$$[\,(\delta^i,(a_1,a_2)),(\delta^n,(z_1,z_2))\,] = (\delta^i,(a_1,a_2))^{-1}(\delta^n,(z_1,z_2))^{-1}(\delta^i,(a_1,a_2))(\delta^n,(z_1,z_2))$$

Since $(\delta^i,(a_1,a_2))^{-1} = (\delta^{-i},(a_1^{-1},a_1^ia_2^{-1}))$ we obtain

$$= (\delta^{-i},(a_1^{-1},a_1^ia_2^{-1}))(\delta^{-n},(z_1^{-1},z_1^nz_2^{-1}))(\delta^{i+n},(a_1,a_2)^{\delta^n}(z_1,z_2))$$

$$= (\delta^{-i-n},(a_1^{-1}z_1^{-1},a_1^{i+n}a_2^{-1}z_1^nz_2^{-1})(\delta^{i+n},(a_1z_1,a_1^na_2z_2))$$

$$= (\delta^0,(a_1^{-1}z_1^{-1}a_1z_1,(a_1^{-1}z_1^{-1})^{i+n}a_1^{i+n}a_2^{-1}z_1^nz_2^{-1}a_1^na_2z_2)$$

$= ((1, (1, z_1^{-i} a_1^n) \in Z(G)$. Hence $G' \leq Z(G)$. In particular choosing $i = 1$ and $a_1 = 1$ we obtain every element of $Z(G)$ is in G'. Hence $Z(G) = G' \cong A$. It follows that $G/Z(G)$ is abelian.

$Z(G/Z(G)) = Z_2(G)/Z(G) = G/Z(G)$ and G is clearly not abelian, it follows that G is nilpotent of class 2.

(b) Assume that G is a torsion group. Then $(\delta^i, (a_1, a_2))$ has finite order for any $i \in \mathbb{Z}$ and $(a_1, a_2) \in A$. Then

$(\delta^i, (a_1, a_2))^n = (1, (1, 1))$. Then

$(\delta^i, (a_1, a_2))(\delta^i, (a_1, a_2))(\delta^i, (a_1, a_2)) \ldots (\delta^i, (a_1, a_2))$

$= (\delta^{2i}, (a_1, a_2))^{\delta^i}, (a_1, a_2))(\delta^i, (a_1, a_2)) \ldots (\delta^i, (a_1, a_2))$

$= (\delta^{2i}, (a_1, a_1^i a_2))(a_1, a_2))(\delta^{2i}, (a_1^2, a_1^i a_2^2)) \ldots (\delta^i, (a_1, a_2))$ implies that $\delta^{ni} = 1$ and $a_1^n = 1$. If order of δ is m, then for any $(a, b) \in A \times A$

$(a, b)^{\delta^m} = (a, b) = (a, a^m b)$ implies $a^m = 1$ for all $a \in A$. In particular A has finite exponent and this exponent is bounded by the order of δ.

Conversely if A has finite exponent say m then $(a, b)^{\delta^m} = (a, a^m b) = (a, b)$ for any $(a, b) \in A \times A$. Hence δ^m is the identity automorphism of $A \times A$. This implies $G = \langle \delta \rangle \ltimes D$ is a torsion group as $D = A \times A$ is a torsion group. In particular $(\delta^i, (a, b))^m$ is an element in $A \times A$ since A has finite exponent we obtain $((\delta^i, (a, b)^m)^n = (1, (1, 1))$.

(c) Let A be the direct product of cyclic groups Z_n for any $n \in \mathbb{N}$. Then by the above observation $G = \langle \delta \rangle \ltimes D$ is a nilpotent group of class 2 .

Since exponent of A is not finite by (b) we obtain that G is not a torsion group. Hence G contains elements of infinite order.

3. SOLUBLE AND NILPOTENT GROUPS

3.1. *Suppose that G is a finite nilpotent group. Then the following statements are equivalent*

(i) *G is cyclic.*

(ii) *G/G' is cyclic.*

(iii) *Every Sylow p-subgroup of G is cyclic.*

Solution: $(i) \Rightarrow (ii)$: Homomorphic image of a cyclic group is cyclic.

$(ii) \Rightarrow (iii)$: Assume that G/G' is cyclic. G is nilpotent so every maximal subgroup of G is normal in G. As G is nilpotent $G' \leq G$. For any maximal subgroup M, $G/M \cong Z_p$ for some prime p. $G' \leq M$ It follows that $G' \leq \bigcap_{M max\ in\ G} M = \Phi(G)$. Now $G/G' = \langle xG' \rangle$. Then $\langle x, G' \rangle = G$ so $\langle x, \Phi(G) \rangle = G$. Hence $\langle x \rangle = G$ as Frattini subgroup is a non-generator group in G. This implies that G is cyclic hence every Sylow subgroup is cyclic.

$(iii) \Rightarrow (i)$ Now assume every Sylow subgroup is cyclic. G is nilpotent hence it is a direct product of its Sylow subgroups $G = O_{p_1}(G) \times O_{p_2}(G) \times \ldots \times O_{p_k}(G)$. Since direct product of Cyclic p-groups of different primes is cyclic we have G is cyclic.

3.2. *Let G be a finite group. Prove that G is nilpotent if and only if every maximal subgroup of G is normal in G.*

Solution: Assume that G is nilpotent. Then every maximal subgroup is normal in G as nilpotent satisfies normalizer condition.

Assume every maximal subgroup of G is normal in G. Let $M_1, M_2, \ldots, M_k$ be the maximal subgroups of G. $M_i \triangleleft G$. $G/M_i \cong Z_p$ for some prime p. Then $G/\bigcap M_i = G/\Phi(G) \hookrightarrow G/M_1 \times G/M_2 \times ... \times G/M_k$ is abelian. Hence $G/\Phi(G)$ is abelian hence $G/\Phi(G)$ is nilpotent. It follows that G is nilpotent.

3.3. *Let p, q, r be primes prove that a group of order pqr is soluble.*

Solution If $p = q = r$, then the group becomes a p-group and hence it is nilpotent so soluble. If $p = q$, then the group has order p^2q these groups are soluble .

So we may assume that p, q, r are distinct primes and $p > q > r$.

Let $|G| = pqr$. Assume that G is the minimal counter example. i.e G is the smallest insoluble group of order pqr. So G has no nontrivial normal subgroup. Because any group of order product of two primes is soluble and extension of a soluble group by a soluble group is soluble. Hence we may assume that G is simple. Let P, Q, R be the Sylow p, q, r subgroups of G respectively and n_p denotes the number of Sylow p-subgroups of G. $n_p \equiv 1 \pmod p$ and n_p divides qr. Since G is simple $n_p \neq 1$ so either $n_p = q$, or $n_p = r$ or $n_p = qr$.

If $n_p = q = |G : N_G(P)|$ we obtain $|N_G(P)| = pr$. Then G acts on the cosets of $N_G(P)$ from right. Then G over kernel of the action say $Ker(\phi)$ is isomorphic to a subgroup of $Sym(q)$. It follows that $|G/Ker(\phi)|$ divides $q!$. Since $p > q$ we obtain $1 \neq Ker(\phi) \lhd G$ contradiction. Similarly $n_p \neq r$. Hence $n_p = qr$. So we have $(p-1)qr$ nontrivial elements of order p.

Now consider Sylow q-subgroups of G. $n_q \equiv 1 \pmod q$ and divides pr. So $n_q = r$ is impossible because if $|G : N_G(Q)| = r$ and r is the smallest prime in p, q, r. So kernel of the action of G on the right cosets of $N_G(Q)$ is nontrivial and our group is simple.

Now we have $(p-1)qr = pqr - qr$ p-elements.

$(q-1)p = pq - p$ at least $pq - p$ q-elements.

r r-elements and identity. So at least $pqr - qr + pq - p + r$ elements. But this number is greater than pqr. This is a contradiction. Hence G is soluble.

3.4. *A nontrivial finitely generated group cannot equal to its Frattini subgroup.*

Solution Let $G = \langle g_1, g_2, \ldots, g_n \rangle$. Assume if possible that $Frat\ G = G$. We may discard any of the g_i if necessary and assume that n is the smallest integer such that $G = \langle g_1, g_2, \ldots, g_n \rangle$. Therefore the subgroup

$K_i = \langle g_1, g_2, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n \rangle$ is a proper subgroup of G. If $Frat\ G = G$, then every element of G is a nongenerator but $\langle K_i, g_i \rangle = G$ and $\langle K_i \rangle \neq G$ which is impossible.

3.5. *Prove that $Frat(Sym(n)) = 1$*

Solution The alternating group $\text{Alt}(n)$ is a maximal subgroup of $(Sym(n))$ as the index of $\text{Alt}(n)$ in $(Sym(n))$ is 2. So Frat $(\text{Sym}(n)) \leq \text{Alt}(n)$. On the other hand $(\text{Sym}(n))$ acts 2-transitively on the set $\Omega_n = \{1, 2, \ldots, n\}$ Because for any (i, j), (k, l) where $i \neq j$ and $k \neq l$ the permutation $(i, k)(j, l)$ takes (i, j) to (k, l). Every 2-transitive group is a primitive permutation group. Hence stabilizer of a point is a maximal subgroup. Hence for any $i \in \Omega_n$ the stabilizer of a point i say $(Sym(\text{n}))_i$ is a maximal subgroup of (Sym(n)) . Hence $Frat((Sym(\text{n}))) \leq \cap_{i=1}^{n}((Sym(\text{n}))_i = 1$. It follows that Frat(Sym(n))= 1.

3.6. *Show that* $Frat(D_\infty) = 1$.

Solution Let $G = \langle x, y \mid x^2 = 1, \quad y^2 = 1\rangle$ Let $a = xy$. Then $G = \langle x, a\rangle, \;\; x^{-1}ax = yx = a^{-1}$. The subgroup generated by an element a is isomorphic to $\mathbb{Z}$ and maximal in G. Hence $D_\infty = \langle a, t\rangle \cong \mathbb{Z} \rtimes \langle t\rangle$ Moreover $\quad x \in \mathbb{Z}$ implies $x^t = x^{-1}$. Then $\langle a^2, t\rangle \lhd D_\infty$, Indeed $t^a = a^{-1}ta = tt^{-1}a^{-1}ta = ta^2 \in \langle a^2, t\rangle$ and $t^{-1}a^2t = a^{-2} \in \langle a^2, t\rangle$, $D_\infty/\langle a^2, t\rangle$ is of order 2. So $\langle a^2, t\rangle$ is a maximal normal subgroup of G. Then $Frat(D_\infty) \leq \langle a\rangle \cap \langle a^2, t\rangle$.

Moreover $\langle a^p, t\rangle$ is a maximal subgroup of D_∞ for any prime p. Since $|D_\infty : \langle a^p, t\rangle| = p$ for any prime p. Then $Frat(D_\infty) \leq \langle a\rangle \cap \langle a^2, t\rangle \cap_p \langle a^p, t\rangle = \langle a\rangle \cap (\cap_{p \text{ prime}} \langle a^p, t\rangle)$. If u is an element in the intersection then $u = a^r$ for some r. Since all primes divide r we obtain $r = 0$. Hence $Frat(D_\infty) = 1$.

3.7. *If G has order $n > 1$, then $|Aut\ G| \leq \prod_{i=0}^{k}(n - 2^i)$ where $k = [log_2(n-1)]$.*

Solution We show that, if $d(G)$ is the smallest number of elements to generate a finite group G, then $|G| \geq 2^{d(G)}$. In particular this says that $d(G) \leq log_2|G| = log_2 n$.

If G is elementary abelian 2-group, then G becomes a vector space over the field $\mathbb{Z}_2$ hence it has a basis consisting of $(0, \ldots, 1, 0 \ldots 0)$. If basis contains k elements, then $|G| = 2^k$. The dimension of a vector space is the smallest number of elements that generate the vector space. Hence $|G| = 2^{d(G)}$ is possible.

Now back to the solution of the problem. Let α be an element in $Aut(G)$. Then α sends generators of G to generators of G. Let $\{x_1, \ldots, x_k\}$ be the smallest set of generators of G. Then by first paragraph $k \leq log_2\ n$ We have $x_1^\alpha \in G$ and order of x_1^α is at least 2, because α is 1-1 and x_1 is a generator. For x_1^α we have at most $n-1$ possibilities. For x_2^α we have $x_2^\alpha \in G \setminus \langle x_1\rangle$. Because if $x_2^\alpha = (x_1^\alpha)^j$ we obtain $x_2^\alpha \in \langle x_1^\alpha\rangle$ but this is impossible as x_2 is a generator and we choose the smallest number of generators. Moreover $x_2^\alpha = (x_1^\alpha)^i$ case may occur as identity but since α is an automorphism this is also impossible.

Hence $x_2^\alpha \in G \setminus \langle x_1^\alpha \rangle$ as order of x_1 is at least 2. Hence for x_2^α we have at most $n-2$ possibilities. For x_3 we have $x_3^\alpha \in G \setminus \langle x_1^\alpha, x_2^\alpha \rangle$, the order of the group $\langle x_1^\alpha, x_2^\alpha \rangle$ is at least 4 hence for x_3^α we have $|G| \setminus 2^2$ possibilities. Continuing like this on the generating set we get the image of G. Observe that α is uniquely determined by its image on the generating set. Hence
$|Aut(G)| \leq (n-1)(n-2)(n-2^2)\dots(n-2^{k-1}) = \prod_{i=0}^{k-1} n - 2^i$.

3.8. *Let G be a finitely generated group. Prove that G has a unique maximal subgroup if and only if G is a nontrivial cyclic p-group for some prime p. Also give an example of a noncyclic abelian group with a unique maximal subgroup.*

Solution Let $G = \langle g_1, g_2, \dots g_n \rangle$. We may assume that if we discard any of the g_i the remaining elements generate a proper subgroup. Then for any i let $H_i = \langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n \rangle$. It is clear that by assumption $g_i \notin H_i$ and H_i is a proper subgroup of G. Let Σ_i be the set of subgroups T of G such that $T \supseteq H_i$ and $g_i \notin T$. Then Σ_i is nonempty since $H_i \in \Sigma_i$ and Σ_i is partially ordered with respect to set inclusion. Then one can show by Zorn's Lemma that Σ_i has a maximal element M_i. Hence $M_i \supseteq H_i$ and $g_i \notin M_i$.The group M_i is a maximal subgroup of G. If x is any element of $G \setminus M_i$ then $\langle M_i, x \rangle > M_i$ hence $g_i \in \langle M_i, x \rangle$ it follows that $\langle M_i, x \rangle = G$, since $\langle H_i, g_i \rangle = G$. So if G is generated by two elements g_1 and g_2, then we may construct two maximal subgroups M_1 and M_2 in G such that $g_i \notin M_i$. Hence it follows that $M_1 \neq M_2$.

So if G has a unique maximal subgroup, then G is a cyclic group. In an infinite cyclic group $\langle a \rangle$ for any prime p, $\langle a^p \rangle$ is a maximal subgroup of $\langle a \rangle$. So if G has a unique maximal subgroup, then G is a finite cyclic group. Then it can be written as a direct product of of its Sylow subgroups. Then for each prime p_i, Sylow p_i subgroup P_i has a unique maximal subgroup M_i. Hence $P_1 \times \dots \times M_i \times P_{i+1} \times \dots \times P_n$ is maximal subgroup of G. It follows that $n = 1$ and hence G is a cyclic p-group for some prime p.

Conversely every cyclic p-group has a unique maximal subgroup is clear because every finite cyclic group G has a unique subgroup for any divisor of the order of G.

$C_{p^\infty} \times \mathbb{Z}_p = G$ is a noncyclic p-group. It is not finitely generated since C_{p^∞} is not finitely generated. But C_{p^∞} is a maximal subgroup of G. Since C_{p^∞} does not have a maximal subgroup C_{p^∞} is the unique maximal subgroup of G.

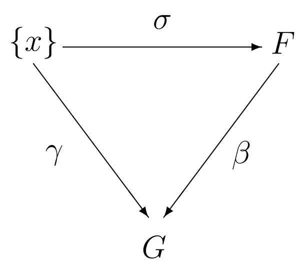
3.9. *Suppose G is an infinite group in which every proper nontrivial subgroup is maximal. Show that G is simple.*

Solution Assume that G is not simple. Let N be a proper normal nontrivial subgroup of G. Then by assumption N is a maximal subgroup of G. It follows that G/N does not have any proper subgroup. Hence it is a finite cyclic group of order p for some prime p.

Let $1 \neq x \in G$. Then $\langle x \rangle$ is a maximal subgroup of G. If x has infinite order, then the group $\langle x^2 \rangle$ is a proper subgroup and by assumption it is maximal. It follows that $G = \langle x \rangle \cong \mathbb{Z}$. But in this group every subgroup is not maximal. Hence G is a torsion group. Again if x has order a composite number then for any prime p dividing order of x the subgroup generated by x^p is a maximal subgroup implies $G = \langle x \rangle$ and so G is a finite cyclic group which is impossible as G is infinite . Hence every element of G is of prime order p. Let $1 \neq x \in N$, then $\langle x \rangle$ is a maximal subgroup implies $N = \langle x \rangle$ and it is of finite order p. Hence G/N and N have finite order. This implies G is a finite group. This contradicts to the assumption that G is an infinite group.

3.10. *A free group is abelian if and only if it is infinite cyclic.*

Solution It is clear that an infinite cyclic group is abelian. It is also free because for any group G and a function $\gamma : X \to G$ say $(x)\gamma = g$

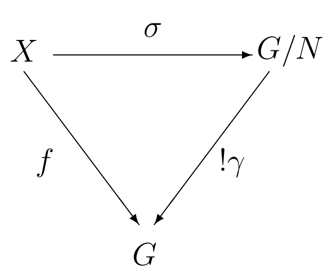


a map β, $(x)\sigma\beta = g$ gives a homomorphism. We may consider σ as identity map hence $(x)\sigma = x$ and $F = \langle x \rangle$. So β becomes a homomorphism from the cyclic group F to the cyclic group $\langle g \rangle$.

Conversely, by the above problem if the rank of a free group is greater than one, then it's center is identity. Hence a free abelian group must have rank one. But indeed a free group of rank one is an infinite cyclic group as every element in the normal form is of type x^i .

3.11. *Let B be a variety. If G is a B-group with a normal subgroup N such that G/N is a free B-group show that there is a subgroup H such that $G = HN$ and $H \cap N = 1$*

Solution Asume that G/N is a free B-group on a set X. We know that the map $\sigma : X \to G/N$ is an injection. Let T be a transversal of N in G. Define a map $f : X \to T \subseteq G$ such that $f(x) = g_x$ where $g_x \in T$ and $\sigma(x) = g_x N$. Since G is a B-group and G/N is a free B-group there exists a unique homomorphism γ such that $f = \sigma\gamma$.



Since γ is a homomorphism $\gamma(G/N) = H$ is a subgroup of G. We now show that H is the required subgroup. Since $\gamma\sigma = f$ and $f(X) = T$ we obtain $H = \langle T \rangle$. Now it is clear that $HN = G$. Now if $y \in H \cap N$, then y can be written as a product of transversals. $y = (yN)\gamma = (N)\gamma = 1$ as γ is a homomorphism. So $y = 1$.

3.12. *Prove that every variety is closed with respect to forming subgroups, images and subcartesian products.*

Solution Let B be a variety and $w = w(x_1, \ldots, x_r)$ be a law of B. Let $G \in B$ and $H \leq G$. Since for any $g_1, \ldots g_r \in G \quad w(g_1, \ldots, g_r) = 1$ in particular for the elements of H we obtain $W(H) = 1$.

Let N be a normal subgroup of $G \in B$. Then

$w(g_1N, \ldots, g_rN) = w(g_1, \ldots, g_r)N = N$. Hence $G/N \in B$

Now let G be a subcartesian product of the groups $G_\lambda \in B$. Let $w = w(x_1, \ldots, x_r)$ and let $i : G \to Cr_{\lambda\in\Lambda}G_\lambda$ be an injection.

For $g_1, \ldots, g_r \in G$ we have $\quad w(g_1, \ldots, g_r)^i = (w(g_1^i, \ldots, g_r^i))_{\lambda\in\Lambda} = (1)_{\lambda\in\Lambda}$ since $G_\lambda \in B$. Since i is an injection this implies $w(g_1, \ldots, g_r) = 1$.

3.13. *Prove that a subgroup which is generated by W-marginal subgroups is itself W-marginal.*

Solution Let W be a nonempty set of words. Recall that a normal subgroup N of G is called W- marginal if for any $g_i \in G$, and $a \in N, \quad w(g_1, \ldots, g_i a, \ldots, g_n) = w(g_1, \ldots, g_n)$. Since the group M generated by normal subgroups is a normal subgroup we need to show that for any element $y \in M$, $w(g_1, \ldots, g_n) = w(g_1, \ldots, g_i y, \ldots, g_n)$. Let $y = a_{i_1}a_{i_2}\ldots a_{i_k}$ where $a_{i_j} \in N_{i_j}$ and N_{i_j} is a W-marginal subgroup of G. Hence for any $g_1, \ldots, g_n \in G$ we have

$w(g_1, \ldots g_j y, \ldots, g_n) = w(g_1, \ldots, g_j a_{i_1}a_{i_2}\ldots a_{i_k}, \ldots, g_n)$. Since N_{i_1} is W-marginal we obtain $w(g_1, \ldots, g_j a_{i_2}\ldots a_{i_k}, \ldots, g_n) = w(g_1, \ldots, g_j a_{i_k}, \ldots, g_n) = w(g_1, \ldots, g_n) = w(g_1, \ldots, g_j, \ldots, g_n)$. Hence M is W-marginal.

3.14. *Prove that $\mathbb{Q}$ is not a subcartesian product of infinite cyclic groups.*

Solution Recall that a group G is subcartesian product of X-groups if and only if G is a residually X-group. So in order to show that $\mathbb{Q}$ is not a subcartesian product of infinite cyclic group we will show that $\mathbb{Q}$ is not residually infinite cyclic group. Assume on the contrary that $\mathbb{Q}$ is residually infinite cyclic. Then for any $0 \neq \frac{m}{n} \in \mathbb{Q}$ there exists $N_{\frac{m}{n}}$ such that $\frac{m}{n} \notin N_{\frac{m}{n}}$ and $\mathbb{Q}/N_{\frac{m}{n}}$ is infinite cyclic. So for any $k \in \mathbb{Z} \quad k.\frac{m}{n} \notin N_{\frac{m}{n}}$. Clearly $\mathbb{Q}$ is not cyclic so there exists $0 \neq \frac{a}{b} \in N_{\frac{m}{n}}$. Hence $ma = bm\frac{a}{b} \in N_{\frac{m}{n}}$. It follows that $\mathbb{Q}/N_{\frac{m}{n}}$ is finite which is a contradiction. On the other hand $ma = an.\frac{m}{n}$.

3.15. *If p and q are distinct primes, prove that a group of order pq has a normal Sylow subgroup. If $p \not\equiv 1 (\mod q)$ and $q \not\equiv 1 (\mod p)$, then the group is cyclic.*

Solution Assume that the prime $p < q$. Let S be a Sylow q-subgroup of G where $|G| = pq$. Then $|G : S| = p$. Number of Sylow q-subgroups n_q is congruent to 1 modulo q. Moreover n_q divides $|G : S| = p$. So $n_q = 1 + kq$ for some $k \in \mathbb{N}$. But $q > p$ implies $n_q = 1$. Hence Sylow q-subgroup S is unique, it follows that S is normal in G.

For the second part consider a Sylow p-subgroup P of G. Let n_p be the number of Sylow p-subgroups. So n_p divides $|G : P| = q$ and $n_p \equiv 1 (\mod p)$. Then $n_p = 1 + kp$ and $1 + kp$ divides q. So n_p is equal to 1 or q. But it is given that $q = n_p \not\equiv 1 (\mod p)$. Hence $n_p = 1$ and P is a normal subgroup of G. $|P| = p$, $|Q| = q$ and $p \neq q$ implies $P \cap Q = 1$. Then for any $x \in P$ and $y \in Q$, $x^{-1}y^{-1}xy \in P \cap Q$. Hence $xy = yx$ for all $x \in P$, $y \in Q$. The group $G = PQ$. G is an abelian group. Assume that $P = \langle x \rangle$ and $Q = \langle y \rangle$, $xy \in G$ and $\langle xy \rangle = \{x^i y^i : \ i \in \mathbb{N} \}$, $(xy)^p = x^p y^p = y^p \neq 1$

$(xy)^q = x^q y^q = x^q \neq 1$ since p does not divide q.

$(xy)^q = x^q y^q = x^q \neq 1$ So $\langle x^q \rangle = \langle x \rangle \leq \langle xy \rangle$ and

$(xy)^p = x^p y^p = y^p \neq 1$ so $\langle y^p \rangle = \langle y \rangle \leq \langle xy \rangle$. Hence p divides $|\langle xy \rangle|$ and q divides $|\langle xy \rangle|$ implies pq divides $|\langle xy \rangle|$. On the other hand $\langle xy \rangle \leq G$ and $|G| = pq$. Hence $\langle xy \rangle = G$ and G is cyclic.

3.16. *Let G be a finite group. Prove that elements in the same conjugacy class have conjugate centralizers. If $c_1, c_2, \ldots, c_n$ are the orders of the centralizers of elements from the distinct conjugacy classes, prove that $\frac{1}{c_1} + \frac{1}{c_2} + \ldots + \frac{1}{c_n} = 1$. Deduce that there exist only finitely many finite groups with given class number h. Find all finite groups with class number 3 or less.*

Solution Let x and x^g be two elements in the same conjugacy class. Then $C_G(x)^g = C_G(x^g)$. Indeed if $y \in C_G(x)^g$, then $y^{g^{-1}} \in C_G(x)$ and $xy^{g^{-1}} = y^{g^{-1}} x$. Taking conjugation of both sides by g gives $x^g y = yx^g$. i.e. $y \in C_G(x^g)$. Hence $C_G(x)^g \subseteq C_G(x^g)$. Similarly $C_G(x^g) \subseteq C_G(x)^g$. Hence $C_G(x^g) = C_G(x)^g$.

By class equation $|G| = \Sigma_{i=1}^{n} |G : C_G(x_i)|$. So $|C_G(x_i)| = |C_G(x_i^g)|$ we have $1 = \Sigma_{i=1}^{n} \frac{1}{|C_G(x_i)|} = \Sigma_{i=1}^{n} \frac{1}{c_i}$.

So $\frac{1}{c_1} + \frac{1}{c_2} + \ldots + \frac{1}{c_n} = 1$.

The set of all groups with only 1 equivalence class satisfy $\frac{1}{c_1} = 1$ where c_1 is the order of the centralizer of identity. Hence $G = \{1\}$.

The set of all groups with two equivalence class satisfy $\frac{1}{c_1} + \frac{1}{c_2} = 1$. Then $c_1 = |C_G(1)| = |G|$. Hence $\frac{1}{c_2} = 1 - \frac{1}{|G|} = \frac{|G|-1}{|G|}$ and so $c_2 = \frac{|G|}{|G|-1}$ $(|G|, |G| - 1) = 1$ implies $|G| - 1 = 1$. Hence $|G| = 2$.

The set of all groups with three equivalence class satisfy $\frac{1}{c_1}+\frac{1}{c_2}+\frac{1}{c_3} = 1$. Since the identity is an equivalence class we have

$$\frac{1}{c_2} + \frac{1}{c_3} = 1 - \frac{1}{|G|} = \frac{|G| - 1}{|G|}.$$

Then $\frac{c_2+c_3}{c_2c_3} = \frac{|G|-1}{|G|}$.

So we obtain $(c_2 + c_3)|G| = c_2c_3(|G| - 1)$. As $(|G|, |G| - 1) = 1$ we have $|G|$ divides c_2c_3. And c_2 divides $|G|$, c_3 divides $|G|$ implies that $(|G| - 1)$ divides $c_2 + c_3$.

First consider the case $c_2 = c_3$. Then $c_2^2((|G|-1) = 2c_2|G|$. Hence $c_2(|G| - 1) = 2|G|$. Since $(|G| - 1)$ divides 2 we obtain $|G| - 1 = 2$. Hence $|G| = 3$ and G is a cyclic group of order 3.

Assume without loss of generality that $c_2 < c_3$. Then $(c_2+c_3)|G| = c_2c_3(|G| - 1)$ implies that

$2c_2|G| \leq (c_2 + c_3)|G| = c_2c_3(|G| - 1) \leq c_3^2(|G| - 1)$ and $(c_2 + c_3)|G| = c_2c_3(|G| - 1) < 2c_3|G|$. It follows that $c_2(|G| - 1) < 2|G|$. By dividing both sides with c_2 we obtain $|G| - 1 < \frac{2}{c_2}|G|$. Then we obtain $|G| < \frac{2}{c_2}|G| + 1$.

c_2 is the order of a centralizer of an element. Hence $c_2 \geq 2$.

If $c_2 > 2$, then $|G| < \frac{2}{c_2}|G| + 1$ is impossible for $|G| \geq 4$. Hence $c_2 = 2$.

Then $(2+c_3)|G| = 2c_3(|G|-1)$ implies that $2|G|+c_3|G| = 2c_3|G|-2c_3$

Then we obtain $c_3|G| = 2|G| + 2c_3$.

But $c_3 > 2$ implies that $(c_3-2)|G| = 2c_3$ and hence $|G| = \frac{2c_3}{c_3-2}$.
If $c_3 = 3$, then $|G| = 6$ and G is isomorphic to S_3.
If $c_3 = 4$, then $|G| = 4$. This is impossible as G is abelian
If $c_3 = 6$, then $|G| = 3$ which is impossible as G is abelian.

If $c_3 > 6$, then $|G| = \frac{2c_3}{c_3-2} \leq 4$. Then we are done as we reach similar groups as above.

3.17. *Let G be a permutation group on a finite set X. If $\pi \in G$ define $Fix(\pi)$ to be the set of fixed points of π that is all $x \in X$ such that $x\pi = x$. Prove that the number of G orbits equals $\frac{1}{|G|}\Sigma_{\pi \in G}|Fix(\pi)|$*

Solution Consider the following set

$$\Omega = \{(x,\pi)|x\pi = x,\ x \in X,\ \pi \in G\}.$$

We count the number of elements in Ω in two ways. First fix an element $x \in X$. Then each x appears as many as $|Stab_G(x)|$ times in Ω. Then $|\Omega| = \Sigma_{x \in X}|Stab_G(x)|$.

Secondly we fix an element $\pi \in G$. Then π appears $Fix(\pi)$ times in Ω. Hence $|\Omega| = \Sigma_{\pi \in G}|Fix(\pi)|$.Then we have $\Sigma_{x \in X}|Stab_G(x)| = \Sigma_{\pi \in G}|Fix(\pi)|$. But we know that $|G : Stab_G(x)|$=length of the orbit of G containing the element x. Let us denote it by $|orbit\ x|$. Hence $|Stab_G(x)| = \frac{|G|}{|Orbit\ x|}$. It follows that $\Sigma_{x \in X}|Stab_G(x)| = \Sigma_{x \in X}\frac{|G|}{|orbit\ x|} = \Sigma_{\pi \in G}|Fix(\pi)|$. On the other hand $\Sigma_{x \in X}\frac{1}{|orbit\ x|}$ =number of orbits of G on X. This is because, if x and y belong to the same orbit, then $|orbit\ x| = |orbit\ y|$. We write X as a disjoint union of orbits say $O_1, \ldots, O_k$. Then

$\Sigma_{x \in X}\frac{1}{|orbit\ x|} = \Sigma_{i=1}^{k}\Sigma_{x \in O_i}\frac{1}{|orbit\ x|} = k$ Since

$\Sigma_{x \in O_i}\frac{1}{|orbit\ x|} = 1$. Hence we have $|G|k = \Sigma_{\pi \in G}|Fix(\pi)|$. Then the number of orbits $k = \frac{1}{|G|}\Sigma_{\pi \in G}|Fix(\pi)|$.

3.18. *Prove that a finite transitive permutation group of order greater than 1 contains an element with no fixed point.*

Solution By previous question we have the formula

$$1 = \frac{1}{|G|}\Sigma_{\pi \in G}|Fix(\pi)|$$

Then we obtain $|G| = \Sigma_{\pi\in G}|Fix(\pi)|$. We know that the identity element of G fixes all points in X. So $|G| = \Sigma_{1\neq\pi\in G}|Fix(\pi)| + |X|$. Since G is transitive on X, for any $y \in X$, $|G : Stab_G(y)| = |X|$. G is a permutation group implies $Stab_G(y) \neq G$. It follows that $|G : Stab_G(y)| = |X| > 1$. Hence the formula $|G| = \Sigma_{1\neq\pi\in G}|Fix(\pi)| + |X|$ and $|Fix(\pi)| \geq 0$ implies there exists a permutation $\pi \in G$ such that $|Fix(\pi)| = 0$ as the sum is over all non-identity elements of G.

Otherwise $Stab_G(y) = G$ for all $y \in X$ Hence G acts trivially on X. But the action is transitive implies $|X| = 1$ But this is impossible as G is a permutation group of order greater than 1.

3.19. *Show that the identity $[u^m, v] = [u, v]^{u^{m-1}+u^{m-2}+\ldots+u+1}$ holds in any group where $x^{y+z} = x^y x^z$. Deduce that if $[u, v]$ belongs to the center of $\langle u, v\rangle$, then $[u^m, v] = [u, v]^m = [u, v^m]$.*

Solution We show the equality by induction on m.

If $m = 1$, then $[u^1, v] = [u, v]$. Assume that

$$[u^{m-1}, v] = [u, v]^{u^{m-2}+u^{m-3}+\ldots+u+1}.$$

Then

$$[u^m, v] = [uu^{m-1}, v] = [u, v]^{u^{m-1}}[u^{m-1}, v]$$

. By induction assumption we obtain

$$[u^m, v] = [u, v]^{u^{m-1}}[u, v]^{u^{m-2}+u^{m-3}+\ldots+u+1}$$

$= [u, v]^{u^{m-1}+u^{m-2}+\ldots+u+1}$. Now if $[u, v]$ belongs to the center of $\langle u, v\rangle$, then

$[u^m, v] = [u, v]^m = [u, v^m]$ as $[u, v]^u = [u, v]^v = [u, v]$

3.20. *A finite p-group G will be called generalized extra-special if $Z(G)$ is cyclic and G' has order p.*

Prove that $G' \leq Z(G)$ and $G/Z(G)$ is an elementary abelian p-group of even rank.

Solution G is a finite p-group, hence nilpotent. Then $\gamma_2(G) = [G, G] = G'$ and $\gamma_3(G) = [G, G'] < G'$ and G' has order p and proper implies $[G, G'] = 1$. It follows that $G' \leq Z(G)$. Then $G/Z(G)$ is an abelian group as $G' \leq Z(G)$. Moreover $[x^p, y] = [x, y]^p$ since $[x, y] \in G' \leq Z(G)$ and $|G'| = p$ implies that $[x^p, y] = [x, y]^p = 1$. Then $x^p \in Z(G)$ for any $x \in G$. This implies $G/Z(G)$ is an elementary abelian p-group. So we may view $G/Z(G)$ as a vector space over a field $\mathbb{Z}_p$. Let m be the dimension of $G/Z(G)$. Define

$$\begin{aligned} f : G/Z(G) \times G/Z(G) \to & \quad \mathbb{Z}_p \\ (xZ(G), yZ(G)) \to & \quad i \end{aligned}$$

where $[x, y] = c^i$ and c is a generator of G'.

Firs we show that f is well defined.

Indeed if $(xZ(G), yZ(G)) = (x'Z(G), y'Z(G))$, then $x = x'z_1$, $y = y'z_2$ where $z_i \in Z(G), i = 1, 2$. Then $[x, y] = [x'z_1, y'z_2] = [x', y']$. So $[x, y] = c^i$ implies $[x', y'] = c^i$.

$f(xZ(G), yZ(G)) = f(x'Z(G), y'Z(G))$. Moreover f is a bilinear form.

$f(x_1x_2Z(G), yZ(G)) = [x_1x_2, y] = [x_1, y]^{x_2}[x_2, y] = [x_1, y][x_2, y]$ as $G' \leq Z(G)$. Moreover

$f(x_1x_2Z(G), yZ(G)) = i+j = f(x_1Z(G), yZ(G))+f(x_2Z(G), yZ(G)$.

and for the other component

$$f(xZ(G), y_1y_2Z(G)) = f(xZ(G), y_1Z(G)) + f(xZ(G), y_2Z(G).$$

Finally we show that f is alternating. Indeed if $xZ(G) \in Rad(f)$, then $f(xZ(G), yZ(G)) = 0$ for all $yZ(G) \in G/Z(G)$ implies $[x, y] = c^0$ for all $y \in G$ i.e $x \in Z(G)$. Hence $xZ(G) = Z(G)$ so $Rad(f) = 0$ implies f is a non-degenerate bilinear form.

Now m is even follows from the linear algebra that if f is a non-degenerate alternating form on a vector space, then the dimension will be even.

3.21. *Let $\mathbb{Q}_p$ be the additive group of rational numbers of the form mp^n where $m, n \in \mathbb{Z}$ and p is a fixed prime. Describe End $\mathbb{Q}_p$ and Aut $\mathbb{Q}_p$.*

Solution Let α be an endomorphism of $\mathbb{Q}_p$. Every element of $\mathbb{Q}_p$ is of the form mp^n for some $m, n \in \mathbb{Z}$. Let $\alpha(1) = kp^m$ for some $k, m \in \mathbb{Z}$ and $\alpha(0) = \alpha(1 - 1) = \alpha(1) + \alpha(-1) = 0$ implies $\alpha(-1) = -kp^m$.

For any integer n, $\alpha(n) = n\alpha(1) = nkp^m$. Now consider $kp^m = \alpha(1) = \alpha(\frac{p^r}{p^r}) = p^r\alpha(\frac{1}{p^r})$ implies that $\alpha(\frac{1}{p^r}) = \frac{kp^m}{p^r} = \frac{\alpha(1)}{p^r}$.

So $\alpha(\frac{i}{p^r}) = \frac{ikp^m}{p^r}$ and we observe that the endomorphism α is determined by $\alpha(1)$

Conversely for any $kp^m \in \mathbb{Q}_p$, the map

$$\begin{array}{ll} \alpha : \mathbb{Q}_p & \to \mathbb{Q}_p \\ \quad x & \to kp^m x \end{array}$$

is an endomorphism of the additive group $\mathbb{Q}_p$. Indeed $\alpha(x+y) = kp^m(x+y) = kp^m x + kp^m y$. Since $kp^m \in \mathbb{Q}_p$ and $x \in \mathbb{Q}_p$, $kp^m x \in \mathbb{Q}_p$. Hence α is an endomorphism. So for any element of $\mathbb{Q}_p$ we may define an endomorphism and for any endomorphism there exists an element of $\mathbb{Q}_p$.

Every automorphism is an endomorphism. So if $\alpha \in Aut\ (G)$, then $\alpha(1) = kp^m$ for some $k, m \in \mathbb{Z}$. Then
$\alpha(\frac{n}{p^r}) = \frac{nkp^m}{p^r}$. So

$$ker(\alpha) = \{\frac{n}{p^r} : \quad \alpha(\frac{n}{p^r}) = 0 \quad \} = \{0\}.$$

For any element $lp^r \in \mathbb{Q}_p$, $\alpha(xp^y) = lp^r$ implies $xkp^m p^y = lp^r$. We need to solve x and y. In particular for $l = 1$, $xkp^m p^y = p^r$ implies that $xt = p^t$. Then k is also a power of p and we can solve x and then solve y accordingly and we obtain automorphisms of $\mathbb{Q}_p$ of the form $\alpha(1) = p^s$ for some $s \in \mathbb{Z}$. Moreover for any α satisfying $\alpha(1) = p^s$ for some $s \in \mathbb{Z}$ we have an automorphism of $\mathbb{Q}_p$. If $\alpha(1) = kp^m$ and $(k,p) = 1$ $\alpha(xp^m) = xkp^{m+y} = lp^r$ where $(l,p) = 1$ $xk = l$ and so $x = \frac{l}{k} \in \mathbb{Z}$ for any l this has a solution if $k = \pm 1$.

3.22. *Prove that a periodic locally nilpotent group is a direct product of its maximal p-subgroups .*

Solution Recall that a periodic locally nilpotent group is a locally finite group, i.e every finitely generated subgroup of G is a finite group. Let Σ be the set of all finite subgroups of G. If S and R are two elements in Σ, then $\langle S, R\rangle \in \Sigma$. Hence $G = \bigcup_{S\in\Sigma} S$. Since for any S in Σ the group S is finite nilpotent implies that S is a direct product of its Sylow p-subgroups.

For a fixed prime p Sylow p-subgroups of S is unique but Sylow p-subgroup of Q is also unique. By Sylow's theorem every p-subgroup of S is contained in a Sylow p-subgroup of Q but there is only one Sylow subgroup of Q implies Sylow p- subgroup of S is contained in a

Sylow p-subgroup of Q. Let $S \leq Q$ and $S, Q \in \Sigma$. Let $P = \bigcup_{S\in\Sigma} P_S$ where P_S is a unique Sylow p subgroup of S.

P is a subgroup of G. Because if $x, y \in P$, then there exist $S_1 \in \Sigma$ and $S_2 \in \Sigma$ such that $x \in P_{S_1}$ and $y \in P_{S_2}$ Then $\langle S_1, S_2\rangle \in \Sigma$ and $P_{\langle S_1,S_2\rangle}$ and $P_{\langle S_1,S_2\rangle} \supseteq P_{S_1}$ and P_{S_2}. Therefore $x, y \in P_{\langle S_1,S_2\rangle}$ and so $xy^{-1} \in P_{\langle S_1,S_2\rangle}$ and $P_{\langle S_1,S_2\rangle} \subseteq P$ hence P is a subgroup. In fact P is a p-subgroup of G. Indeed the above argument shows that every finitely generated subgroup of P is contained in a subgroup P_S for some $S \in \Sigma$.

P is a maximal subgroup. If there exists $P_1 > P$, then let $x \in P_1 \backslash P$, the element x is a p-element, hence $\langle x\rangle \in \Sigma$ Then $\langle x\rangle = P_{\langle x\rangle} \subseteq P$

The group P is normal in G, since for any $g \in G$ and $x \in P$ there exists an $S \in \Sigma$ such that $x \in P_S$ and the group $\langle S, g\rangle \in \Sigma$ and $x \in P_{\langle S,g\rangle}$. Since $P_{\langle S,g\rangle} \lhd \langle S, g\rangle$ we obtain $g^{-1}xg \in P_{\langle S,g\rangle} \subseteq P$. This is true for any prime p. Hence all maximal subgroups of G are normal for any prime p. Since every element $g \in G$ is contained in a finite group $S \in \Sigma$ and S is a direct product of its Sylow subgroups . We obtain $G = \prod_p P$.

4. SYLOW THEOREMS AND APPLICATIONS

4.1. *Let S be a Sylow p-subgroup of the finite group G. Let $S \cap S^g = 1$ for all $g \in G \setminus N_G(S)$. Then $|Syl_p(G)| \equiv 1 \ (\mod |S|)$.*

Solution: By Sylow's theorems $|Syl_p(G)| = |G : N_G(S)|$ and any two Sylow p-subgroup of G are conjugate in G and $|Syl_p(G)| \equiv 1($mod $p)$. The group S acts by right multiplication on the set $\Omega = \{N_G(S)x | x \in G\}$ of right cosets of $N_G(S)$ in G. Now we look to the lengths of the orbits of S on Ω. As $S \leq N_G(S)$, $N_G(S)S = N_G(S)$. Hence the orbit of S containing $N_G(S)$ is of length 1. $N_G(S)xS = N_G(S)x$ implies $N_G(S)xSx^{-1} = N_G(S)$ i.e, $xSx^{-1} \leq N_G(S)$. But then xSx^{-1} and S are both Sylow p-subgroups of $N_G(S)$, and there exists only one Sylow p-subgroup of $N_G(S)$. This implies that $xSx^{-1} = S$, i.e., $x \in N_G(S)$.

Moreover the length of the orbit of S on Ω is equal to $|S : Stab_S(N_G(S))x|$.

$N_G(S)xs = N_G(S)x$ implies $xsx^{-1} \in N_G(S)$. Then $s \in N_G(S^x)$. But s is a p-element, $\langle s\rangle$ normalizes S^x implies $\langle s\rangle S^x$ is a subgroup,

S^x is a Sylow p-groups implies $\langle s\rangle S^x = S^x$ i.e. $s \in S^x$. But then $s \in S \cap S^x = 1$. Hence $N_G(S)xs \neq N_G(S)x$ for all non-trivial cosets of $N_G(S)$ in G. Then the length of the orbit of S on Ω is $|S|$.

$|\Omega| = 1 + k|S|$, i.e, $|\Omega| \equiv 1(\mod |S|)$.

4.2. *Show that a group G of order $90 = 2.3^2.5$ is not simple.*

Solution Let n_i denote the number of Sylow i subgroups of G. Let S_i denote a Sylow i subgroup of G. If $n_5 = 1$, then S_5 is a normal subgroup of G and $|G/S_5| = 2.3^2$. Hence it follows that G is soluble. If $n_5 = 6$, then consider n_3. If $n_3 = 1$, then $S_3 \lhd G$ and $|G/S_3| = 2.5$. So G/S_3 is soluble and S_3 is soluble implies that G is soluble and we are done. So assume if possible that $n_3 = 10$. If the intersection of two Sylow 3-subgroup is the identity, then we have 8.10 elements of order 3 and 24 elements of order 5 so we obtain 105 elements which is impossible. Hence there exists Sylow 3-subgroups P and Q such that $1 \neq P \cap Q \neq$ the groups P and Q. Moreover $|P \cap Q| = 3$ and $P \cap Q \lhd \langle P, Q\rangle$. Then $|PQ| \geq \frac{|P||Q|}{|P\cap Q|} = \frac{81}{3} = 27$. So $|\langle P, Q\rangle| \geq 27$. So if $|\langle P, Q\rangle| = 45$ and so G is soluble. If $\langle P, Q\rangle = G$, then $P \cap Q \lhd G$ implies $|G/(P \cap Q)| = 2.3.5$ is soluble hence we obtain G is soluble.

4.3. *Show that a group of order 144 is not simple.*

Solution Assume that G is simple. Let S_3 be a Sylow 3-subgroup of G. The number of Sylow 3-subgroups $n_3 = 4$ implies that $|G : N_G(S_3)| = 4$. Then G acts on the right cosets of $N_G(S_3)$. This implies that there exists

$$\phi \ : \ G \to Sym(4)$$

Then $G/Ker(\phi)$ is isomorphic to a subgroup of $Sym(4)$. But $|Sym(4)| = 24$ and $|G| = 144$. Then $Ker(\phi) \neq 1$. Then $G/Ker(\phi)$ is soluble as $Sym(4)$ is soluble.

We may assume that $n_3 = 16$. If any two Sylow 3-subgroup intersect trivially, then $8.16 = 128$ hence we have only one Sylow 2-subgroup. It follows that G is soluble. So there exists Sylow 3-subgroups P and Q such that $1 \neq P \cap Q$. So $|P \cap Q| = 3$. Then $P \cap Q \lhd \langle P, Q\rangle$. Then $|PQ| \geq 27$ implies that $|\langle P, Q\rangle| \geq 36$. Hence $|G/\langle P, Q\rangle| = 4$. Then as in the first paragraph we obtain $G/Ker(\phi)$ is isomorphic to a subgroup of $Sym(4)$ and $|Ker(\phi)| \leq 36$ soluble implies G is soluble. Hence we obtain G is not simple.

4.4. *Prove that*
(a) every group of order $3^2.5.17$ *is abelian.*
(b) Every group of order $3^3.5.17$ *is nilpotent.*

Solution Let G be group of order $3^2.5.17$ and let n_p denotes the number of Sylow p subgroups of G. By Sylow's theorem $n_p \equiv 1 \pmod p$ and $n_p = |G : N_G(P)|$.

$n_{17} \equiv 1 \pmod{17}$ and n_{17} divides $3^2.5$ implies $n_{17} = 1$. This implies that Sylow 17-subgroup of G is unique and hence normal in G.

Let Q be a Sylow 5-subgroup. Then $n_5 = 1$ or 51 and $n_5 = |G : N_G(Q)|$ Since Sylow 17-subgroup R is normal in G we obtain $RQ \leq G$. The group Q is a Sylow 5-subgroup of RQ. Since $|RQ| = 5.17$ Sylow 5-subgroup is unique in RQ. That implies $|RQ : N_{RQ}(Q)| = 1$. i.e. $N_{RQ}(Q) = RQ$. Then $N_{RQ}(Q) \leq N_G(Q)$. Therefore $|N_G(Q)| \geq |RQ| = 5.17$. Therefore $|G : N_G(Q)| \leq 3^2$ and n_5 cannot be equal to 51. It follows that $n_5 = 1$. So Sylow 5-subgroup Q is normal in G. Let S be a Sylow 3-subgroup of G. Then $n_3 = 1,$ or 85. Since $RS \leq G$ and S is a Sylow 3-subgroup of RS $4, 7, 10,$ does not divide 17. Then Sylow 3-subgroup is unique in RS. It follows that $RS = N_{RS}(S) \leq N_G(S)$. And $|N_G(S)| \geq 17.3^2$. So $n_3 = |G : N_G(S)| \leq 5$. So Sylow 3-subgroup of G is normal in G. Hence all Sylow subgroups of G are normal. Then G is nilpotent. Hence G is a direct product of its Sylow subgroups.

Since any group of order p^2 is abelian we obtain S is an abelian group and Q and R are cyclic. Hence G is an abelian group.

(b) Every group of order $3^3.5.17$ is nilpotent.

Let $G = 3^3.5.17$. Then $n_{17} = 1$ so Sylow 17-subgroup is normal in G, say R. By the same argument above Sylow 5-subgroup is unique and so normal in G say Q.

Let S be a Sylow 3-subgroup. It is unique in RS hence $n_3 = |G : N_G(S)| \leq 5$ and $n_3 \equiv 1 \pmod 3$ and n_3 does not divide 5 implies S is unique. Hence G is nilpotent. Therefore $G = S \times Q \times R$ where $|S| = 3^3$.

A group G is called a **supersoluble** group if G has a series of normal subgroups $N_i \lhd G$ in which each factor N_i/N_{i+1} in the series is cyclic for all i. The group A_4 is soluble but not a supersoluble group.

4.5. *Prove that the product of two normal supersoluble groups need not be supersoluble.*

Hint: Let X be a subgroup of $GL(2,3)$ generated by

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Thus $X \cong D_8$. Let X act in the natural way on $A = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ and write $G = X \ltimes A$. Show that G is not supersoluble. Let L and M be the disjoint Klein 4-subgroups of X and consider $H = LA$ and $K = MA$.

Solution Observe that $|a| = 4,\ |b| = 2$, and $b^{-1}ab = a^{-1}$. Then $|X/\langle a\rangle| = 2, \quad |X| = 8$. Let $D_8 = \langle x, y\rangle$. Then

$$\begin{aligned} \phi \ :\ & D_8 \to X \\ & x \to a \\ & y \to b \end{aligned}$$

By Von Dyck's theorem ϕ is a homomorphism. Since ϕ is onto, $|X| = 8$, we obtain ϕ is an isomorphism.

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} -j \\ i \end{pmatrix}$$

So $G = X \ltimes A$ and $|G| = 72$. Moreover G has a series $G \rhd A \rhd 1$, $G/A \cong D_8$.

If G is supersoluble, then there exists a normal subgroup of G contained in A. Let J be such a normal subgroup of order 3. Arbitrary element of J is of the form $\begin{pmatrix} a \\ b \end{pmatrix}$. Then J is invariant under the action of X. Let

$$J = \{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -a \\ -b \end{pmatrix} \}$$

Then

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix} \notin J$$

Therefore G is not supersoluble.

Let

$$L = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \}$$

and

$$M = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \}$$

Then $\langle L, M \rangle = X = LM$ and $H = LA, K = MA$ implies $|LA| = |MA| = 36$. The groups H, K are normal in G hence $HK = G$ since $HK \geq \langle A, L, M, X \rangle = G$. The groups H, K are supersoluble.

$$J = \{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} a \\ a \end{pmatrix}, \begin{pmatrix} -a \\ -a \end{pmatrix} \}$$

J is invariant under the action of L.

$H \triangleright L_1 \triangleright A \triangleright J \triangleright 1$ so L is supersoluble.

$$B = \{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix} \}$$

is invariant under the action of M. $B \triangleleft K$

$K \triangleright K_1 \triangleright A \triangleright B \triangleright 1$. Hence K is supersoluble.

4.6. *Let $G = GL(2,3)$ and $G_1 = SL(2,3)$.*

(a) Find $|G|$ and $|G_1|$. Moreover show that $|G/G_1| = 2$ and $|Z(G)| = 2$ and $Z(G) \leq G_1$

(b) Show that $G_1/Z(G) \cong Alt(4)$ and that G_1 has a normal Sylow 2-subgroup say J.

(c) Show that J is nonabelian. Deduce that $G_1' = J$.

(d) Deduce that $G' = G_1$. Hence G_1 has derived length 3 and G has derived length 4.

Solution (a) $|G| = (3^2-1)(3^2-3) = 8.6 = 48$. Consider determinant homomorphism $det : G \to Z_3^* = \{1, -1\}$. Then $Ker\ (det) = G_1$ and $G/G_1 \cong \{1, -1\}$. Hence $|G_1| = 24 = 3.2^3$.

$$Z(G) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\} \leq G_1$$

(b) Sylow 3-subgroup of G (and G_1) has order 3. Then

$$U_1 = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, x \in \mathbb{Z}_3\}, \quad \text{and } U_2 = \{\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, y \in \mathbb{Z}_3\}$$

are Sylow 3-subgroups. $n_3 \equiv 1 \pmod 3$ and $n_3 = |G_1 : N_{G_1}(U_1)|$. Since the number of Sylow 3-subgroups is greater than or equal to 2 and $n_3 = |G_1 : N_{G_1}(U_1)|$ we obtain $n_3 = 4$ and $|N_{G_1}(U_1)| = 6$. Since $Z(G) \leq N_{G_1}(U_1)$ we obtain $N_{G_1}(U_1)$ is a cyclic subgroup of order 6 as Sylow 2-subgroup is in the center and any group of order 6 is either isomorphic to S_3 or cyclic group of order 6. Then G_1 acts by right multiplication on the set of right cosets of $N_{G_1}(U_1)$ in G_1. The homomorphism $\phi : G_1 \to Sym(4)$ gives; $G_1/Ker\ \phi$ is isomorphic to a subgroup of $Sym(4)$. Then $Ker\ \phi = \cap_{x \in G_1} N_{G_1}(U_1)^x$. As $Z(G) \leq Ker\ \phi$ and

$$N_{G_1}(U_1) \cap N_{G_2}(U_2) = \{ \begin{pmatrix} a & c \\ 0 & a \end{pmatrix}\} \cap \{\begin{pmatrix} x & 0 \\ z & x \end{pmatrix} \} \leq Z(G_1)$$

we obtain $Z(G_1) = Ker\ \phi$.

$G_1/Z(G_1)$ is isomorphic to a subgroup of $Sym(4)$. Since $Sym(4)$ has only one subgroup of order 12 we obtain $G_1/Z(G_1) \cong Alt(4)$.

The group $Alt(4)$ has a normal subgroup of order 4, we have $J/Z(G_1) \lhd G_1/Z(G_1) \cong Alt(4)$ and we obtain $|J/Z(G_1)| = 4$ and $|J| = 8$, Sylow 2-subgroup J of G_1 is a normal 2-subgroup.

Moreover $J/Z(G)$ *char* $G_1/Z(G) \lhd G/Z(G)$ implies $J/Z(G) \lhd G/Z(G)$. Hence $J \lhd G$. In fact

$$J = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$$

(c) Observe that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

So J is non-abelian.

For $G_1' = J$; as $J \lhd G_1$ and $G_1/J \cong \mathbb{Z}_3$ we obtain $G_1' \leq J$ and $J' \neq 1$ as J is non-abelian. Then $J/Z(G_1) \leq G_1/Z(G_1) \cong Alt(4)$. Then J is non-abelian of order 8, implies that $J'' = 1$ and $J' \leq Z(G_1)$. Recall that$(1 \lhd V \lhd Alt(4), \quad Alt(4)'' = 1)$.

The order $|G_1'Z(G_1)/Z(G_1)| = 4$ implies $G_1' \neq 1$ and $G_1'' \leq Z(G_1)$. So $G_1^{(3)} = 1$. If $G_1' = J$ we are done. Now $|G_1'| = 2$ or $|G_1'| = 4$. $|G_1'| = 2$ implies G_1 is nilpotent hence Sylow 3-subgroup is unique which is impossible as we already found two distinct Sylow 3-subgroup.

If $|G_1'| = 4$, then Sylow 2-subgroup is a quaternion group of order 8 implies that G_1' is cyclic. Hence $|Aut(G_1')| = 2$. Therefore $G_1/C_{G_1}(G_1')$ is isomorphic to a subgroup of $Aut(G_1')$. Since $N_{G_1}(G_1') = G_1$ and 3 divides $|C_G(G_1')|$ we obtain Sylow 3-subgroup is unique in $C_{G_1}(G_1') \lhd G_1$. Then Sylow 3-subgroup is unique in G_1 This is a contradiction. Hence $G_1' = J$.

As $[1 + xe_{12}, ye_{11} - ye_{22}] = 1 - 2xe_{12}$ and $[1 + xe_{21}, ye_{11} - ye_{22}] = 1 + 2xe_{21}$ we obtain U_1 and U_2 are contained in G'. And hence the subgroup $\langle U_1, U_2 \rangle \leq G'$. Then the elements of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & x \\ y & 1 \end{pmatrix} \in G'$$

In particular for $x = y = 1$ the elements

$$a = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \in G'$$

$|a| = 4$ and for $x = y = -1$

$$b = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \in G'$$

is an element of order 4. Moreover a and b are contained in J. Since these elements generate J we obtain $J \leq G'$. Hence 3 divides $|G'|$ and 8 divides $|G'|$ and $G' \leq G_1$ implies that $|G'| = 24$ and $G' = G_1$.

4.7. *Let G be a finite group with trivial center. If G has a non-normal abelian maximal subgroup A, then show that $G = AN$ and $A \cap N = 1$ for some elementary abelian p-subgroup N which is minimal normal in G. Also A must be cyclic of order prime to p.*

Solution Let A be an abelian maximal subgroup of G such that A is not normal in G. Then for any $x \in G \backslash A$. So we obtain $\langle A, x\rangle = G$. Therefore for any $x \in G\backslash A$, we have $A^x \neq A$ otherwise A would be normal in G. But then consider $A \cap A^x$. Since $A^x \neq A$ and A is maximal, $\langle A, A^x\rangle = G$. If $w \in A \cap A^x$, then $C_G(w) \geq \langle A, A^x\rangle = G$. Since A is abelian and A^x is isomorphic to A so that A^x is also maximal and abelian in G. But $C_G(w) = G$ implies $w \in Z(G) = 1$. Hence $A \cap A^x = 1$. This shows that A is Frobenius complement in G. Hence there exists a Frobenius kernel N such that $G = AN$ and $A \cap N = 1$. By Frobenius Theorem, Frobenius kernel is a normal subgroup of G. So $G = AN$ implies $G/N = AN/N = A/A \cap N$, hence G is soluble. It follows from the fact that minimal normal subgroup of a soluble group is elementary abelian p-group for some prime p, N is an elementary abelian p-group.

If there exists a normal subgroup M in G such that $G = AM$ and $M \leq N$. Then $A \cap M \leq A \cap N = 1$. Moreover $|G| = \frac{|A||M|}{|A\cap M|} = \frac{|A||N|}{|A\cap N|} = |A||M| = |A||N|$. Hence $|M| = |N|$, this implies $M = N$. Hence N is minimal normal subgroup of G.

Since N is elementary ableian p-group if A contains an element g of order power of p, then the group $H = N\langle g\rangle$ is a p-group. Hence $Z(H) \neq 1$. Let $x \in Z(H)$. If $x \in A$, then $C_G(x) \geq \langle A, N\rangle = G$. This implies that $x \in Z(G) = 1$ which is impossible. So $x \in G\backslash A$. Then $\langle g\rangle \cap \langle g\rangle^x \leq A \cap A^x = 1$. But $\langle g\rangle \cap \langle g\rangle^x = \langle g\rangle$. Hence $(|A|, p) = 1$. i.e. $p \nmid |A|$.

Claim: A is cyclic: By Frobenius Theorem, Sylow q-subgroups of Frobenius complement A are cyclic if $q > 2$ and cyclic or generalized quaternion if $p = 2$ (Burnside Theorem, Fixed point free Automorphism in [**1**]). Since A is abelian Sylow subgroup can not be generalized quaternion group. Hence all Sylow subgroups of A are cyclic. This implies that A is cyclic.

4.8. *Let G be a finite group. If G has an abelian maximal subgroup, then show that G is soluble with derived length at most 3.*

Solution Let A be an abelian maximal subgroup of G. If A is normal in G, then for any $x \in G \backslash A$, we have $A\langle x\rangle = G$. Hence $G/A \cong A\langle x\rangle/A \cong x\rangle/\langle x\rangle \cap A$. Then G/A is cyclic and A is abelian implies $G'' = 1$ and hence G is soluble. Now consider $Z(G)$. If $Z(G)$ is not a subgroup of A, then $AZ(G) = G$. This implies that G is abelian. Hence we may assume that $Z(G)$ is a subgroup of A. Then $A \cap A^x \geq Z(G)$, on the other hand if $w \in A \cap A^x$, then $C_G(w) \geq \langle A, A^x\rangle = G$. Hence $w \in Z(G)$. It follows that $A \cap A^x = Z(G)$.

Now, consider the group $\bar{G} = G/Z(G)$. Then $\bar{G}$ has an abelian maximal subgroup $\bar{A}$. Then for any $\bar{x} \in \bar{G} \backslash \bar{A}$. We obtain $\bar{A} \cap \bar{A}^x = \bar{1}$. Hence $\bar{G}$ is a Frobenius group with Frobenius complement $\bar{A}$ and Frobenius kernel $\bar{N}$. Then $\bar{G} = G/Z(G) = (A/Z(G))(N/Z(G))$. The group $\bar{G}$ is soluble hence G is soluble. As in [**1**] Lemma 2.2.8 $\bar{N}$ is an elementary abelian p-group and $\bar{N}$ is a minimal normal subgroup of $\bar{G}$.

Since $\bar{G} = \bar{A}\bar{N}$ and A is abelian, we obtain $\bar{G}' \leq \bar{N}$ and $\bar{G}'' \leq Z(\bar{G})$ as $\bar{N}$ is abelian. Hence $(G/Z(G))' \leq N/Z(G)$ and $G''Z(G)/Z(G) \leq Z(G)/Z(G)$. i.e $G'' \leq Z(G)$. Hence $G^{(3)} = 1$.

4.9. *Let α be a fixed point free automorphism of a finite group G. If α has order a power of a prime p, then p does not divide $|G|$. If $p = 2$, infer via the Feit-Thompson Theorem that G is soluble.*

Solution: Recall that a fixed point free automorphism α stabilizes a Sylow p-subgroup of G. The point is $P_0^\alpha = P_0^g$ for some $g \in G$ where P_0 is a Sylow p-subgroup of G. Since the map

$$\begin{array}{rl} G \to & G \\ x \to & x^{-1}x^\alpha \end{array}$$

is a bijective map we may write every element $g = h^{-1}h^\alpha$ for some $h \in G$. Let $P = P_0^{h^{-1}}$. Then

$$P^\alpha = ((P_0^{h^{-1}})^\alpha = (P_0^\alpha)^{(h^{-1})^\alpha} = (P_0^g)^{(h^{-1})^\alpha} = (P_0^{h^{-1}h^\alpha})^{(h^{-1})^\alpha} = P^{h^\alpha (h^{-1})^\alpha} = P$$

So α becomes an automorphism of P. Then let $H = P \rtimes \langle\alpha\rangle$. If $\langle\alpha\rangle$ is a p-group, then H is a p-group. So $Z(H) \neq 1$. This implies that if $1 \neq Z(H)$, then $z^\alpha = z$ which is impossible by fixed point free action. Hence α can not be a power of a prime dividing $|G|$. i.e. $(|\alpha|, |G|) = 1$.

So if a group G has a fixed point free automorphism of order 2^n for some n, then $(2, |G|) = 1$. Hence by Feit-Thompson theorem $|G|$

is odd and G is soluble. It follows that a group has a fixed point free automorphism α of order power of a prime 2 is soluble.

4.10. *If X is a nontrivial fixed point free group of automorphisms of a finite group G, then $X \ltimes G$ is a Frobenius group.*

Solution: We need to show that for any

$$\alpha \in (X \ltimes G) \setminus X, \qquad X \cap X^{\alpha} = 1.$$

Let $\alpha = xg$ where $g \neq 1$ and assume that $w \in X \cap X^{\alpha} = X \cap X^{xg} = X \cap X^{g}$. Then $w = x = y^{g}$ for some $x, y \in X$. The element $yy^{-1}g^{-1}yg = x = w \in X$ implies that $y^{-1}g^{-1}yg = y^{-1}x \in X$ as $x, y \in X$. Moreover $y(g^{-1})^{y}g = x \in GX$. Then $(g^{-1})^{y}g \in X \cap G = 1$. Hence $(g^{-1})^{y}g = 1$ which implies $(g^{-1})^{y} = g^{-1}$. But y is a fixed point free automorphism, this implies that $g = 1$ which is a contradiction.

Hence $X \cap X^{\alpha} = 1$ for all $\alpha \in (X \ltimes G) \setminus X$. It follows that $X \ltimes G$ is a Frobenius group with Frobenius Kernel G and Frobenius complement X.

4.11. *A soluble p-group is locally nilpotent.*

Solution: A group G is called a p-group if every element of G has order a power of a fixed prime p. A periodic soluble group is a locally finite group. One can see this by induction on the derived length n of G. For $n = 1$, then G is a periodic abelian group which is clearly locally nilpotent. Assume $n > 1$ and let S be a finitely generated subgroup of G. Then SG'/G' is finite as it is abelian and finitely generated p-group. Moreover $SG'/G' \cong S/S \cap G'$. As S is finitely generated and $S/(S \cap G')$ is finite we have $S \cap G'$ is a finitely generated subgroup of the p-group G'. By induction assumption $S \cap G'$ is finite and $S/S \cap G'$ is finite implies S is finite. It follows that G is locally finite.

A locally finite p-group is locally nilpotent because every finitely generated subgroup is a finite p-group. Hence it is nilpotent.

4.12. *A finite group has a fixed-point-free automorphism of order 2 if and only if it is abelian and has odd order.*

Solution: Let G be an abelian group of odd order.

$$\alpha : G \to G$$

$$x \to x^{-1}$$

α is a fixed-point-free automorphism of G. Indeed if $\alpha(x) = x$ implies $x = x^{-1}$. Then $x^2 = 1$. Hence there exists a subgroup of order 2. This implies $|G|$ is even. Hence $x = 1$.

Conversely let α be a fixed point free automorphism of a finite group G. Then the map

$$\beta : G \to G$$
$$x \to x^{-1}\alpha(x)$$

is a $1-1$ map. Indeed $\beta(x) = \beta(y)$ implies $x^{-1}\alpha(x) = y^{-1}\alpha(y)$. Then $yx^{-1} = \alpha(y)\alpha(x)^{-1} = \alpha(yx^{-1})$. Since α is fixed-point-free we obtain $x = y$. Now, for any $g \in G$, there exists $x \in G$ such that $g = x^{-1}\alpha(x)$. Then $\alpha(g) = \alpha(x^{-1}\alpha(x)) = \alpha(x)^{-1}\alpha^2(x) = \alpha(x)^{-1}x = g^{-1}$. Now $\alpha(g_1g_2) = (g_1g_2)^{-1} = \alpha(g_1)\alpha(g_2) = g_1^{-1}g_2^{-1} = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$. It follows that $g_1g_2 = g_2g_1$. Hence G is an abelian group.

Moreover if there exists an element y of order 2, then $\alpha(y) = y^{-1} = y$. Which is impossible as α is a fixed-point-free automorphism of order 2.

4.13. *Let G be a finite Frobenius group with Frobenius kernel K. If $|G : K|$ is even, prove that K is abelian and has odd order.*

Solution: Frobenius kernel K is a normal subgroup of G. Let X be a Frobenius complement. Then $G = KX$ and $K \cap X = 1$. Since order of G/K is even, we obtain $|G/K| = |XK/K| = |X/X \cap K| = |X|$. Then there exists an element $x \in X$ of order 2. Then

$$\alpha_x : K \to K$$
$$g \to x^{-1}gx.$$

is an automorphism of K. Moreover $|\alpha_x| = 2$ and α_x is fixed-point-free.

If $x^{-1}kx = k$ for some $k \in K$. Then $kxk^{-1} = x$ and $X \cap X^k \neq 1$ where $k \in G \setminus X$. Which is impossible. Hence α_x is a fixed point free automorphism of K of order 2. Then by question 4.12 K is abelian of odd order.

Recall that if G is a finite group and $p_1, \cdots, p_k$ denote the distinct prime divisors of $|G|$ and Q_i is a Hall p_i'-subgroup of G. Then the set $\{Q_1, \cdots, Q_k\}$ is called a Sylow system of G. By Hall's theorem every soluble group has a Sylow-system. $N = \bigcap_{i=1}^{k} N_G(Q_i)$ is called system normalizer of G.

4.14. *Locate the system normalizers of the groups:*
(a) S_3 ***(b)*** A_4 ***(c)*** S_4 ***(d)*** $SL(2,3)$

Solution:

(a) S_3 is soluble and $H_1 = \{(1),(12)\}$, $H_2 = \{1,(13)\}$, $H_3 = \{1,(23)\}$. are Hall 2-subgroups of S_3 or Hall $3'$-subgroup of S_3, and $A_3 = \{1,(123),(132)\}$ is a Hall $2'$-subgroup or Hall 3-subgroup of S_3. Then $\{H_1, A_3\}$ is a Sylow system of G. $N_{S_3}(H_i) \cap N_{S_3}(A_3) = H_i \cap S_3 = H_i$ system normalizer of S_3 $i = 1,2,3$.

(b) Observe that $V = \{1,(12)(34),(13)(24),(14)(23)\}$ is a Hall 2-subgroup or Hall $3'$-subgroup of A_4. The group $V \lhd A_4$, hence there is only one Hall 2-subgroup of A_4.

$$H_1 = \{(1),(123),(132)\}, H_2 = \{(1),(124),(142)\},$$

$$H_3 = \{(1),(134),(143)\}, H_4 = \{1,(234),(243)\}$$

are Hall 3-subgroups or Hall $2'$-subgroups of A_4.

Since A_4 has no subgroup of index 2 and H_i is not normal in A_4 we obtain $N_{A_4}(H_i) = H_i$. $\{H_i, V\}$ is Sylow System of A_4 and $N_{A_4}(H_i) \cap N_{A_4}(V) = H_i \cap A_4 = H_i$, System normalizers of A_4.

(c) S_4 is a soluble group of derived length 3. Sylow 2-subgroup becomes Hall 2-subgroup or equivalently Hall $3'$-subgroup.

Sylow 3-subgroup of S_4 becomes Hall 3-subgroup equivalently Hall $2'$-subgroup of S_4. Let H_1 be a Sylow 2-subgroup of order 8 in S_4. Then H_1 is not normal in S_4. Hence $N_{S_4}(H_1) = H_1$. There are 4 Sylow 3-subgroups. Hence $K_1 = \{1,(123),(132)\}$ as in A_4 every 3-cycle generates a Sylow 3-subgroup of S_4. But $|S_4 : N_{S_4}(K_i)| = 4$ implies $|N_{S_4}(K_i)| = 6$.

Namely $N_{S_4}(K_1) \cong S_3$. Similarly $N_{S_4}(K_i) \cong S_3$. For K_1 we obtain $N_{S_4}(K_1) = \{1,(13),(12),(23),(123),(132)\}$, $\{K_1, H_1\}$ is a Sylow System. Since $V \lhd S_4$ every Sylow 2-subgroup contains V.

$$H_1 = \{1,(12),(34),(13)(24),(14)(23),(23),(1342),(1243),(14)\}$$

$N_{S_4}(H_1) \cap N_{S_4}(K_1) = H_1 \cap S_3 = \{(1), (23)\}$ system normalizer of S_4.

(d)

$$|SL(2,3)| = \frac{(3^2-1)(3^2-3)}{2} = \frac{8 \cdot 6}{2} = 24.$$

$$H_1 = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \middle| x \in \mathbb{Z}_3 \right\} \quad \text{is a Sylow 3-subgroup}$$

$$H_2 = \left\{ \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \middle| y \in \mathbb{Z}_3 \right\} \quad \text{is a Sylow 3-subgroup}$$

$$H_3 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, y = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, y^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$

is a Sylow 3-subgroup of $SL(2,3)$.

Then the number of Sylow 3-subgroups is 4.

$$Z(SL(2,3)) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

$N_{SL(2,3)}(H_1) \geq \ \langle Z(SL(2,3)), H_1 \rangle = H_1 \times Z(SL(2,3))$

The index $|SL(2,3) : N_{SL(2,3)}(H_1)| = 4$ implies $|N_{SL(2,3)}(H_1)| = 6$. So $N_{SL(2,3)}(H_1)$ is a cyclic group of order 6 and generated by the element

$$t = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$

All Sylow 2-subgroup contains $Z(SL(2,3))$. Let S be a Sylow 2-subgroup of order 8. Then $N_{SL(2,3)}(S) = SL(2,3)$ since by Question 4.6 S is normal in $SL(2,3)$, $\{S, H_1\}$ is a Sylow system.

$$N_{SL(2,3)}(S) \cap N_{SL(2,3)}(H_1) = Z(SL(2,3)) \times H_1.$$

So $Z(SL(2,3)) \times H_1$ is a System normalizer of $SL(2,3)$.

4.15. *Let G be a finite soluble group which is not nilpotent but all of whose proper quotients are nilpotent. Denote by L the last term of the lower central series. Prove the following statements:*

(a) *L is minimal normal in G.*

(b) *L is an elementary abelian p-group.*

(c) *there is a complement $X \neq 1$ of L which acts faithful on L*

(d) *the order of X is not divisible by p.*

Solution: **(a)** Let $\gamma_1(G) \geq \gamma_2(G) \geq \cdots > \gamma_k(G) = L \neq 1$. Since G is not nilpotent, there exists k such that $L = \gamma_k(G) = \gamma_{k+1}(G) \neq 1$. The group L is a normal subgroup of G as each term in the lower central series is a characteristic subgroup of G. If there exists a normal subgroup $N \lhd G$, and $N \leq L$, then by assumption G/N is a nilpotent group. Hence $\gamma_n(G/N) = 1$. Equivalently $\gamma_n(G/N) \leq N$. But this implies $N/N = \gamma_n(G/N) = \gamma_n(G)N/N = L/N$. This implies $L = N$ contradiction. Hence L is a minimal normal subgroup of G.

(b) For a finite soluble group minimal normal subgroup is an elementary abelian p-group for some prime p.

(c) Now by Gaschutz-Schenkman, Carter Theorem, if G is a finite soluble group and L is the smallest term of the Lower central series of G. If N is any system normalizer in G, then $G = NL$. If in addition L is abelian, then also $N \cap L = 1$ and N is a complement of L.

Now by the above theorem L has a complement N where N is a system normalizer in G. For solvable groups system normalizer exists. Hence there exists X such that $G = XL$. By the same theorem since L is abelian we obtain $X \cap L = 1$, so X is a complement of L in G.

Claim X acts faithfully on L.

Since L is a minimal normal subgroup of G, the group X acts on L by conjugation. Let K be the kernel of the action of X on L. Then $K \lhd X$ and K commutes with L. Hence $N_G(K) \geq XL = G$. It follows that K is normal in G. Then G/K is nilpotent by assumption. Hence $L = \gamma_n(G) \leq K \leq X$. But $X \cap L = 1$. Hence $K = 1$ and X acts on L faithfully.

(d) Assume that $p|\,|X|$. Let P be a Sylow p-subgroup of G containing L. Then for $x \in P \setminus L$ and $x \in X$, $\langle x \rangle$ acts an L faithfully. Consider $T = L\langle x \rangle$. Then T is a p-group $Z(T) \neq 1$. Let $1 \neq w \in Z(T)$, $w = \ell x^i$ for some i. Then for any $g \in L$, $g^{\ell x^i} = g^{x^i} = g \quad \text{as} \quad L \quad \text{is abelian}.$

Then x^i acts trivially on L implies $x^i = 1$. This implies $Z(T) \leq L$. X system normalizer is nilpotent, implies that $G = XL$.

Let $X = P_1 \times P_2 \times \cdots \times P_n$, where P_i's are Sylow p_i-subgroups of X. Let $LP_1 = P$ Sylow p-subgroup of G.

Since $G = LX$ and $P_1 \lhd X$ we obtain $N_G(P) = G$ so $P \lhd G$. Then $Z(P)$ char $P \lhd G$ so $Z(P) \lhd G$. Then $G/Z(P)$ is nilpotent hence $L = \gamma_n(G) \leq Z(P)$. So $[L, P_1] = 1$. Since X normalizes P_1 and $[L, P_1] = 1$ we obtain $P_1 \lhd G$. If $P_1 \neq 1$, then G/P_1 is nilpotent. Hence $L = \gamma_n(G) \leq P_1$ but $L \cap P_1 = 1$. Hence $L \leq P_1$ is impossible. So $P_1 = 1$.

4.16. *Write H asc K to mean that H is an ascendant subgroup of a group K. Establish the following properties of ascendant subgroups.*

(a) *H asc K and K asc G imply that H asc G.*

(b) *H asc $K \leq G$ and L asc $M \leq G$ imply that $H \cap L$ asc $K \cap M$*

(c) *If H asc $K \leq G$ and α is a homomorphism from G, then H^α is asc K^α. Deduce that HN asc KN if $N \lhd G$.*

Solution: **(a)** H asc K implies, there exists a series $H = H_0 \lhd H_1 \lhd \cdots \lhd H_\alpha = K$ for some ordinal α. Similarly there exists an ordinal β such that $K = K_0 \lhd K_1 \lhd \cdots \lhd K_\beta = G$. Then

$$H = H_0 \lhd H_1 \cdots \lhd H_\alpha = K \lhd K_{\alpha+1} \lhd \cdots \lhd K_{\alpha+\beta} = G$$

be an ascending series of H in G.

(b) Let $L = L_0 \lhd H_1 \lhd \cdots \lhd L_\beta = M$ be a series of L in M. Then

$$L \cap H = L_0 \cap H \lhd L_1 \cap H \lhd \cdots \lhd L_\beta \cap H = M \cap H$$

Moreover

$$M \cap H \lhd M \cap H_1 \lhd \cdots \lhd M \cap H_\alpha = M \cap K$$

Hence $L \cap H$ asc $M \cap K$.

(c) If H asc K, then there exists an ordinal γ such that $H = H_0 \lhd H_1 \lhd \cdots \lhd H_\gamma = K$. Then $H^\alpha \leq H_1^\alpha \leq \cdots \leq H_\gamma^\alpha = K^\alpha$ is an ascending series of H^α in K^α.

$HN = H_0N \lhd H_1N \lhd \cdots \lhd H_\gamma N = KN$. Hence HN asc KN. Observe that $H \lhd H_1$ and $N \lhd G$ implies $HN \lhd H_1N$

4.17. *A group is called radical if it has an ascending series with locally nilpotent factors. Define the upper Hirsch Plotkin series of a group G to be the ascending series $1 = R_0 \leq R_1 \leq \ldots$ in which $R_{\alpha+1}/R_\alpha$ is* *the Hirsch-Plotkin radical of G/R_α and $R_\lambda = \bigcup_{\alpha \langle \lambda} R_\alpha$ for limit ordinals λ. Prove that the radical groups are precisely those groups which coincide with a term of their upper Hirsch-Plotkin series.*

Solution: It is clear by definition of a radical group that, if a group coincides with a term of its upper Hirsch Plotkin series then it is an ascending series with locally nilpotent factors. Hence it is a radical group.

Conversely assume that G is a radical group with an ascending series $1 \leq H_0 \leq H_1 \leq \cdots \leq H_\beta = G$ such that $H_i \lhd H_{i+1}$ and H_{i+1}/H_i is locally nilpotent.

Recall from [**1**, 12.14] that if G is any group the Hirsch-Plotkin radical contains all the ascendent locally nilpotent subgroups.

Let R_i denote i^{th} term in Hirsch-Plotkin series of G.

Claim: $H_i \leq R_i$ for all i. For $i = 0$ clear.

Assume that $H_{i-1} \leq R_{i-1}$ we know that H_i/H_{i-1} is locally nilpotent. Then $H_iR_{i-1}/R_{i-1} \leq G/R_{i-1}$. Moreover H_iR_{i-1}/R_{i-1} is an ascendent subgroup of G/R_{i-1} and H_iR_{i-1}/R_{i-1} is locally nilpotent. Hence by [**1**, 12.1.4] it is contained in the Hirsch Plotkin radical of G/R_{i-1} i.e. $H_iR_{i-1} \leq R_i$. It follows that $H_i \leq R_i$.

4.18. *Show that a radical group with finite Hirsch-Plotkin radical is finite and soluble.*

Solution: Let H be a Hirsch-Plotkin radical of a radical group G. By previous question $C_G(H) = Z(H)$. Now consider $G/C_G(H) = G/Z(H)$ which is isomorphic to a subgroup of Aut H. If H is finite, then Aut H is finite. Hence $G/Z(H)$ is a finite group. Hence $G/Z(H)$ is finite and H is finite implies G is a finite group. Then $1 \leq H_1 \leq H_2 \leq \cdots \leq H_n = G$ implies G is soluble as $\gamma_k(H_n) \leq H_{n-1}$. So $G^{(k)} \leq H_{n-1}$ and so on.

4.19. $T(2, \mathbb{Z}) \cong D_\infty \times \mathbb{Z}_2$ *where D_∞ is the infinite dihedral group.*

Solution:

$$T(2, \mathbb{Z}) = \left\{ \begin{bmatrix} \mp 1 & t \\ 0 & \mp 1 \end{bmatrix} \middle| t \in \mathbb{Z} \right\}$$

$$C = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\} \text{ is equal to the center of } T(2,\mathbb{Z}).$$

Indeed $\begin{bmatrix} a & c \\ 0 & b \end{bmatrix}$ is in the $Z(T(2,\mathbb{Z}))$

$$\begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & t \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & t \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a & c \\ 0 & b \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} a & at-c \\ 0 & -b \end{bmatrix} = \begin{bmatrix} a & c+tb \\ 0 & -b \end{bmatrix}, \quad \forall t \in \mathbb{Z}$$

$at - c = c + tb \Rightarrow (a-b)t = 2c$ Since t is arbitrary

for $t = 0$ we have $c = 0$ and so $a = b$

Hence the center $C \cong \mathbb{Z}_2$.

Now consider

$$H = \langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbb{Z} >$$

H is a subgroup of $T(2,\mathbb{Z})$

$$N = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbb{Z} \right\} \leq H$$

$$N \cong \mathbb{Z}$$

$$\varphi : N \to \mathbb{Z}$$

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \to b$$

$$\varphi\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \right) = \varphi\left(\begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \right) = a + b$$

$$\varphi\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \right) + \varphi\left(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right) = a + b \Rightarrow \varphi \text{ is a homomorphism}$$

$N \lhd H$. Indeed

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}^{-1} \in N$$

$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ is an element of order 2.

So $H = N \rtimes \langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \rangle$ Let $a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Every element of N is inverted by a and $a^2 = 1$. The group N is a cyclic group isomorphic to $\mathbb{Z}$. So, H is isomorphic to infinite dihedral group.

{ The dihedral group D_∞ is a semidirect product of infinite cyclic group and a group of order 2 }. $H \cap C = \{1\}$

$[H, C] = 1$

$H \times C \leq T(2, \mathbb{Z})$

We take an arbitrary element from $T(2, \mathbb{Z})$. If the entry $a_{11} = -1$ by multiplying

$$\begin{bmatrix} -1 & b \\ 0 & \mp 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -b \\ 0 & \mp 1 \end{bmatrix} \in H$$

Therefore, every element in $T(2, \mathbb{Z})$ can be written as a product of an element from H.

4.20. *Show that $Q_{2^n}/Z(Q_{2^n})$ is isomorphic to $D_{2^{n-1}}$ for $n > 2$.*

Solution: Recall that

$$Q_{2^n} = \langle x, y \mid x^2 = y^{2^{n-2}}, y^{2^{n-1}} = 1, x^{-1}yx = y^{-1},\ n > 2 \rangle$$

$(y^{2^{n-2}})^x = (y^{-1})^{2^{n-2}} = (x^2)^x = x^2 y^{2^{n-2}}$ as $y^{2^{n-2}}$ has order 2. So $y^{2^{n-2}}$ commutes with x and y hence $y^{2^{n-2}}$ is in the center of Q_{2^n}. The group $\langle y \rangle$ has index 2 in Q_{2^n} as $x^2 \in \langle y \rangle$. Hence $\langle y \rangle$ is normal in Q_{2^n}. Moreover $x\langle y \rangle \neq \langle y \rangle$ and $|Q_{2^n}| = 2^n$ and every element of Q_{2^n} can be written as $x^i y^j$ where $i = 0, 1$ and $0 \leq j \lneqq 2^{n-1}$.

The writing of every element is unique, as

$$x^i y^j = x^m y^k,\ \ 0 \leq i, m \leq 1,\ \ 0 \leq k, j \leq 2^{n-1}$$

implies $x^{m-i} = y^{k-j}$. Then $m - i = 0$ or 1 but if $m - i = 1$ we obtain $x \in \langle y \rangle$ which is impossible. Hence $m - i = 0$ and $k - j = 0$. This implies every element of Q_{2^n} can be written uniquely in the form $x^i y^j$.

Now assume that an element $x^i y^j \in Z(Q_{2^n})$. Then $(x^i y^j)^x = x^i (y^j)^x = x^i y^{-j} = x^i y^j$. Hence $y^{2j} = 1$. Since there exists a unique subgroup of order 2 in $\langle y \rangle$ we obtain $j = 2^{n-2}$. Then

$(x^i y^{2^{n-2}})^y = (x^i)^y y^{2^{n-2}} = y^{-1} x^i y y^{2^{n-2}}$

$= x^i x^{-i} y^{-1} x^i y y^{2^{n-2}} = x^i (y^{-1})^{x^i} y y^{2^{n-2}} = x^i y^{2^{n-2}}$.

It follows that $(y^{-1})^{x^i} y = 1$ and so $(y)^{x^i} = y$. Since $i = 0$ or 1, in case $i = 1$ we obtain $y^2 = 1$ and $Q_{2^n} = Q_4$ abelian case.

So the center $Z(Q_{2^n}) = \langle y^{2^{n-2}} \rangle$ and $|Z(Q_{2^n})| = 2$. Moreover $|Q_{2^n}/Z(Q_{2^n})| = 2^{n-1}$.

$$Q_{2^n}/Z(Q_{2^n}) = \langle x, y \mid x^2 = y^{2^{n-2}}, y^{2^{n-1}} = 1,\ x^{-1}yx = y^{-1} > /Z(Q_{2^n}).$$

Let $\overline{x} = x\ Z(Q_{2^n}$ and $\overline{y} = y\ Z(Q_{2^n})$. Then $\overline{x}^2 = 1$ and $\overline{y}^{2^{n-2}} = 1$. Moreover $\overline{x}^{-1}\overline{yx} = \overline{y}^{-1}$.

The map

$$\varphi : Q_{2^n}/Z(Q_{2^n}) \longrightarrow D_{2^{n-1}}$$

where

$$D_{2^{n-1}} = \langle a, b \mid a^2 = 1 = b^{2^{n-2}}, a^{-1}ba = b^{-1} \rangle.$$

$$\overline{x} \longrightarrow a$$

$$\overline{y} \longrightarrow b$$

φ is an epimorphism both groups have the same order hence $Q_{2^n}/Z(Q_{2^n}) \cong D_{2^{n-1}}$

4.21. *Let $G = \langle x, y \mid x^3 = y^3 = (xy)^3 = 1 \rangle$. Prove that $G \cong A \ltimes < t >$ where $t^3 = 1$ and $A = \langle a \rangle \times \langle b \rangle$ is the direct product of two infinite cyclic groups, the action of t being $a^t = b$, $b^t = a^{-1}b^{-1}$.*

Hint: prove that $\langle xyx, x^2y \rangle$ is a normal abelian subgroup.

Solution: Let $N = \langle xyx, x^2y \rangle$. The group N is a normal subgroup of G. Indeed, $x^{-1}(xyx)x = yx^2 = yx^{-1}$.

The product of two elements of N is $xyx \cdot x^2y = xy^2 = xy^{-1} = (yx^{-1})^{-1} = (yx^2)^{-1} \in N$ hence $yx^{-1} \in N$

$x(xyx)x^{-1} = x^2y \in N$

$(x^2y)^x = x^{-1}x^2yx = xyx \in N$, and $x(x^2y)x^{-1} = yx^{-1} \in N$. Hence $N \lhd G$.

By previous paragraph $xyx \cdot x^2y = xy^2 = xy^{-1}$ and now

$$x^2y \cdot xyx = x \cdot (xy)(xy) \cdot x = x \cdot (xy)^2 \cdot x = x \cdot y^2x^2 \cdot x = xy^2 = xy^{-1}.$$

Hence x^2y and xyx commute.

Observe that

$$xy \cdot xy = (xy)^{-1} = y^{-1}x^{-1} = y^2x^2.$$

Hence N is abelian normal subgroup of G. For the order of the element xyx we have

$$(xyx)^2 = xyx \cdot xyx = xyx^2yx = xyx^{-1}yx$$

Since $xy^{-1} \in N$ we obtain $xN = yN$. But $x^3 = 1$ implies $x^3N = N$. It is clear that $x \notin N$; otherwise $N = G$, then G is abelian, but $xy \neq yx$, $\langle xN \rangle$ has order 3; otherwise $x^2 \in N$ implies $y \in N$ as $yx^2 \in N$. So xN has order 3 and $\langle x \rangle \cap N = 1$

$$(x^2y)^x = x^{-1}x^2yx = xyx$$

Moreover

$$(xyx)^x = yx^2 = y^{-1}(x^{-2}x^{-1})y^{-1}x^{-1} \text{ as } y^3 = 1 \text{ and } x^2 = x^{-1}$$

$$= y^{-2}x^{-1} = yx^{-1} = yx^2 = (x^2y)^{-1}(xyx)^{-1} \text{as } y^{-2} = y \text{ and } x^2 = x^{-1}$$

Now let $x^2y = a$, and $xyx = b$. Then
$a^x = (x^2y)^x = x^{-1}x^2yx = xyx$ and

$$b^x = (xyx)^b = yx^2 = (x^2y)^{-1} = y^{-1}x^{-2}x^{-1}y^{-1}x^{-1}$$

$$= y^{-2}x^{-1} = yx^{-1} = yx^2 = a^{-1}b^{-1}.$$

Then by von Dyck's theorem we obtain the isomorphism.

4.22. *Show that S_3 has the presentation*

$$\langle x, y \mid x^2 = y^3 = (xy)^2 = 1 \rangle$$

Solution: Let $G = \langle x, y \mid x^2 = y^3 = (xy)^2 = 1 \rangle$. Then $(xy)^2 = xyxy = 1$. This implies $xyx = y^{-1} = x^{-1}yx$ as $x^2 = 1$. Hence the subgroup generated by y is a normal subgroup of order 3. Let $N = \langle y \rangle$. Since G is generated by x and y, $G = \langle x, N \rangle$, $N \lhd G$ implies $|G| \leq 6$ on the other hand $x^iy^j = x^ry^s$ implies $x^{-r+i} = y^{s-j} \in \langle x \rangle \cap \langle y \rangle = 1$ as $|\langle x \rangle| = 2$ and $|\langle y \rangle| = 3$. This implies

$x^{i-r} = 1$ i.e. $x^i = x^r$ and $y^s = y^j$. Hence two possibilities for i and three possibilities for j implies we have 6 elements of the form $x^i y^j$. Hence $|G| = 6$.

Recall that $S_3 = \langle (12), (123) \rangle$

$(12)(123)(12) = (132) = (123)^{-1}$

$(12)(123)(12)(123) = (132)(123) = 1.$

Now let $\alpha = (12)$, $\beta = (123)$. Then every relation in G holds in S_3. So by Von Dycks Theorem there exists an epimorphism

$$\begin{aligned} \varphi \quad S_3 &\longrightarrow \quad G \\ x &\longrightarrow \quad \alpha \\ y &\longrightarrow \quad \beta \end{aligned}$$

$$\begin{aligned} Ker(\varphi) &= \{\alpha^i \beta^j) \mid \varphi(\alpha^i \beta^j) = x^i y^j = 1\} \\ &= \{\alpha^i \beta^j) \mid x^i = y^{-j} \in \langle x \rangle \cap \langle y \rangle = 1\} \\ &= \{1\}. \end{aligned}$$

Hence $G \cong S_3$

4.23. *Let G be a finite group with trivial center. If G has a non-normal abelian maximal subgroup A, then $G = AN$ and $A \cap N = 1$ for some elementary abelian p-subgroup N which is minimal normal in G. Also A must be cyclic of order prime to p.*

Solution: Let A be an abelian maximal subgroup of G such that A is not normal. Then for any $x \in G \backslash A$. So we obtain $\langle A, x \rangle = G$. Therefore for any $x \in G \backslash A$, we have $A^x \neq A$ otherwise A would be normal in G. But then consider $A \cap A^x$. Since $A^x \neq A$ and A is maximal, $\langle A, A^x \rangle = G$. If $w \in A \cap A^x$, then $C_G(w) \geq \langle A, A^x \rangle = G$. Since A is abelian and A^x is isomorphic to A so that A^x is also maximal and abelian in G. But $C_G(w) = G$ implies $w \in Z(G) = 1$. Hence $A \cap A^x = 1$. This shows that A is Frobenius complement in G. Hence there exists a Frobenius kernel N such that $G = AN$ and $A \cap N = 1$. By Frobenius Theorem, Frobenius kernel is a normal subgroup of G. So $G = AN$ implies $G/N = AN/N = A/A \cap N$, hence G is soluble as Frobenius kernel N is nilpotent. It follows from the fact that minimal normal subgroup of a soluble group is elementary abelian p-group for some prime p N is an elementary abelian p-group.

If there exists a normal subgroup M in G such that $G = AM$ and $M \leq N$. Then $A \cap M \leq A \cap N = 1$. Moreover $|G| = \frac{|A||M|}{|A \cap M|} = \frac{|A||N|}{|A \cap N|} =$

$|A||M| = |A||N|$. Hence $|M| = |N|$, this implies $M = N$. Hence N is minimal normal subgroup of G.

Since N is elementary abelian p-group if A contains an element g of order power of p, then the group $H = N\langle g\rangle$ is a p-group. Hence $Z(H) \neq 1$. Let $x \in Z(H)$. If $x \in A$, then $C_G(x) \geq \langle A, x\rangle = G$. This implies that $x \in Z(G) = 1$ which is impossible. So $x \in G\backslash A$. Then $\langle g\rangle \cap \langle g\rangle^x \leq A \cap A^x = 1$. But $\langle g\rangle \cap \langle g\rangle^x = \langle g\rangle$. Hence $(|A|, p) = 1$. i.e. $p \nmid |A|$.

Now we show that A is cyclic. Indeed by Frobenius Theorem, Sylow q-subgroups of Frobenius complement A are cyclic if $q > 2$ and cyclic or generalized quaternion if $p = 2$ (Burnside Theorem, Fixed point free Automorphism in [**1**]). Since A is abelian Sylow subgroup can not cannot be generalized quaternion group. Hence all Sylow subgroups of A are cyclic. This implies that A is cyclic.

4.24. *Let G be a finite group. If G has an abelian maximal subgroup, then G is soluble with derived length at most 3.*

Solution: Let A be an abelian maximal subgroup of G. If A is normal in G, then for any $x \in G\backslash A$, we have $A\langle x\rangle = G$. Hence $G/A \cong A\langle x\rangle/A \cong \langle x\rangle/\langle x\rangle \cap A$. Then G/A is cyclic and A is abelian implies $G'' = 1$.

Consider $Z(G)$. If $Z(G)$ is not a subgroup of A, then $AZ(G) = G$. This implies that G is abelian. Hence we may assume that $Z(G)$ is a subgroup of A. Then $A \cap A^x \geq Z(G)$, on the other hand if $w \in A \cap A^x$, then $C_G(w) \geq \langle A, A^x\rangle = G$. Hence $w \in Z(G)$. It follows that $A \cap A^x = Z(G)$.

Now, consider the group $\bar{G} = G/Z(G)$. Then $\bar{G}$ has an abelian maximal subgroup $\bar{A}$. Then for any $\bar{x} \in \bar{G}\backslash\bar{A}$. We obtain $\bar{A} \cap \bar{A}^x = \bar{1}$. Hence $\bar{G}$ is a Frobenius group with Frobenius complement $\bar{A}$ and Frobenius kernel $\bar{N}$. Then $\bar{G} = G/Z(G) = (A/Z(G))(N/Z(G))$. The group $\bar{G}$ is soluble hence G is soluble. As in [**1**, Lemma 2.2.8] $\bar{N}$ is an elementary abelian p-group and $\bar{N}$ is a minimal normal subgroup of $\bar{G}$.

Since $\bar{G} = \bar{A}\bar{N}$ and A is abelian, we obtain $\bar{G}' \leq \bar{N}$ and $\bar{G}'' \leq Z(\bar{G})$ as $\bar{N}$ is abelian. Hence $(G/Z(G))' \leq N/Z(G)$ and $G''Z(G)/Z(G) \leq Z(G)/Z(G)$. i.e $G'' \leq Z(G)$. Hence $G''' = 1$.

4.25. *Let M be a maximal subgroup of a locally finite group G. If M is inert and abelian, then G is soluble.*

Solution: If M is normal, then for any $x \in G\backslash M$, we have $\langle M, x\rangle = G$ implies that $G/M = \langle x\rangle M/M \cong \underbrace{\langle x\rangle/\langle x\rangle \cap M}_{abelian}$.

Then $[G, G] \leq M$. So $[G, G]$ is abelian. Therefore, $G \geq [G, G] \geq 1$. So that G is soluble of derived length 2.

Assume M is not normal in G. Then $N_G(M) = M$ as M maximal. Then for any $x \in G\backslash M$ we have $M^x \neq M$. Hence $\langle M, M^x\rangle = G$. By inertness we have $|M : M \cap M^x| < \infty$ and $|M^x : M \cap M^x| < \infty$. Then by [**?**, Belyaev's Paper] this implies that $|G : M \cap M^x| = |\langle M, M^x\rangle : M \cap M^x| < \infty$. So $M \cap M^x \ntrianglelefteq G$. Indeed, $N_G(M \cap M^x) \geq \langle M, M^x\rangle = G$. Then the group $G/M \cap M^x$ is a finite group with abelian maximal subgroup, then by [**1**, Theorem 2.2.1] $G/M \cap M^x$ is soluble. It follows that G is soluble as $M \cap M^x$ is abelian.

4.26. *Let G be soluble and $\Phi(G) = 1$. If G contains exactly one minimal normal subgroup N, then $N = F(G)$.*

Solution: Let N be a minimal normal subgroup of the soluble G. Then N is an elementary abelian group and so it is a normal nilpotent subgroup of G. Hence $N \leq F(G)$.

The group $F(G)$ is a characteristic nilpotent subgroup of G so

$$F(G) = O_{p_1}(F(G)) \times \ldots \times O_{p_k}(F(G))$$

where each $O_{p_i}(F(G)) \lhd G$ and G contains only one minimal normal subgroup implies that, there exists only one prime p.

$Z(F(G)) char F(G) char G$ implies there exists a minimal normal subgroup in $Z(F(G))$. Uniqueness of N implies every element of order p in $Z(F(G))$ is contained in N. So $\Omega_1(Z(F(G))) \leq N$. Moreover every maximal subgroup of $F(G)$ is contained in a maximal subgroup of G. Hence $\Phi(F(G)) \leq \Phi(G) = 1$. Then

$$F(G) \cong F(G)/\Phi(F(G)) \to Dr\ F(G)/M_i$$

M_i is maximal in $F(G)$. Since each $F(G)/M_i$ is cyclic of order p we obtain $F(G))$ is an elementary abelian p group. Then $\Omega_1(Z(F(G))) \leq N$ implies $F(G) \leq N$ and hence we have the equality $F(G) = N$.

4.27. *Let G be a group of order $2n$. Suppose that half of the elements of G are of order 2 and the other half form a subgroup H of order n. Prove that H is of odd order and H is an abelian subgroup of G.*

Solution: Since H is a subgroup of index 2 in G we have H is a normal subgroup of G. There is only one coset of H in G other than itself say xH is the second coset and $xH \neq H$. Hence by assumption every element in xH has order 2. In particular G/H is of order 2 and x is an element of G of order 2. Then for any $h \in H$ we have $(xh)^2 = (xh)(xh) = 1$. It follows that $xhx = x^{-1}hx = h^{-1}$ as x has order 2. Then the inner automorphism i_x is of order 2 and inverts every element $h \in H$. Then for any $h_1, h_2 \in H$ we have $x^{-1}(h_1h_2)x = (h_1h_2)^{-1} = h_2^{-1}h_1^{-1} = (x^{-1}h_1x)(x^{-1}h_2x) = h_1^{-1}h_2^{-1}$. Hence $h_2^{-1}h_1^{-1} = h_1^{-1}h_2^{-1}$ for all $h_1, h_2 \in H$. By taking inverse of each side we have $h_1h_2 = h_2h_1$. Hence H is abelian. If $|H|$ is even, then by Cauchy theorem there will be an element of order 2 in H. But then there will be $n+1$ elements of order 2 in G which is impossible. Hence H is a subgroup of odd order.

4.28. *Show that $Sym(6)$ has an automorphism that is not inner, $Out(Sym(6)) \neq 1$*

Solution: (a) We first show that there is a faithful, transitive representation of $Sym(5)$ of degree 6.

First we show that there exists a subgroup of $Sym(5)$ of order 20 hence the index $|Sym(5) : G| = 6$. Then the action of $Sym(5)$ on the right cosets of G is

$$\gamma : Sym(5) \hookrightarrow Sym(6), \gamma \text{ is faithful and transitive on 6 letters.}$$

Let

$$G = \{f_{a,b} : GF(5) \to GF(5) \mid f_{a,b}(x) = ax + b \text{ where } a, b \in GF(5) \text{ and } a \neq 0\}$$

Then we may consider G as a subgroup of $Sym(5)$ as each element being a permutation on 5 elements. Then $G \leq Sym(5)$ and $|G| = 20$ as there are 4 choices for a and 5 choices for b. Therefore $|Sym(5) : G| = 6$. Then $Sym(5)$ acts on the right cosets of G in $Sym(5)$ by right multiplication.

Then we may write the element of G as permutations of 5 elements and then G contains both even and odd permutations. For example, $f_{2,2}$ corresponds to the permutation of $GF(5)$ as $2x+2$. Then $f_{2,2} = (1,4,0,2)$ so $f_{2,2}$ defines an odd permutation. On the other hand

$$f_{1,1} \ : \ (1,2,3,4,0) \text{ which is an even permutation and}$$
$$f_{2,0} \ : \ (1,2,4,3) \text{ which is an odd permutation.}$$

If K is the kernel of the action of $Sym(5)$ on the cosets of G in $Sym(5)$, then $K \trianglelefteq Sym(5)$. Since the kernel of the action is $\cap_{x\in Sym(5)} G^x$ which lies inside G and $G \lneqq Sym(5)$ and the only normal subgroup of $Sym(5)$ is either $Alt(5)$ or $\{1\}$. Since $|K| \leq |G| \lneqq |Alt(5)|$, we have $K = \{1\}$. Hence $Sym(5)$ acts faithfully and transitively on the set of cosets of G in $Sym(5)$ where degree of the action is 6.

(b) The groups $Sym(6)_1, Sym(6)_2, \ . \ . \ . \ , Sym(6)_6$ which are mutually conjugate and isomorphic to $Sym(5)$, but these subgroups fixes a point as a subgroup of $Sym(6)$.

The symmetric group $Sym(6)$ has a subgroup $H \cong Sym(5)$ which is transitive on 6 elements.

$Sym(5)$ has 6 Sylow 5-subgroups. Indeed the number of Sylow 5-subgroups $n_5 \equiv 1 \pmod 5$ so it can be $1, 6, 11, 16$ or 21 and moreover $n_5 | 24 = |Sym(5) : N_{Sym(5)}(C_5)|$ implies that $n_5 = 6$ as we have 6 Sylow subgroup and so Sylow 5-subgroup is not normal in $Sym(5)$. So $Sym(5)$ acts on the set of Sylow 5-subgroups by conjugation. Hence there exists a homomorphism

$$\varphi : Sym(5) \hookrightarrow Sym(6)$$

representing members of $Sym(5)$ as permutation of Sylow 5-subgroups. Kernel of the action is either Alternating group $Alt(5)$ or $\{1\}$. Kernel cannot be $Alt(5)$ since the set of the Sylow 5-subgroups of $Sym(5)$ are also the set of Sylow 5-subgroups of $Alt(5)$ and $Alt(5)$ can act on this set transitively. Hence the kernel of the action is $\{1\}$. Hence $H = Im(\varphi) \cong Sym(5)$ and $Im(\varphi) \leq Sym(6)$ and $Im(\varphi)$ acts transitively and faithfully on the set of Sylow 5-subgroups. One can observe that the subgroup G of order 20 corresponds to $N_{Sym(5)}(C_5)$

and recall that $N_{Sym(5)}(C_5)$ does not lie in $Alt(5)$ as it contains odd and even permutations.

(c) Let

$$\pi_1 : Sym(6) \hookrightarrow Sym\{Sym(6)_1y_1, Sym(6)_1y_2, ..., Sym(6)_1y_6\}$$

The natural representation of $Sym(6)$ on the cosets of $Sym(6)_1$ gives an isomorphism

$$\begin{array}{ccc} Sym(6) & \hookrightarrow & \pi_1(Sym(6)) \\ \sigma & \longrightarrow & \pi_1(\sigma) \end{array}$$

The representation of $Sym(6)$ on the cosets of $H = Im(\varphi) \cong Sym(5)$ is faithful since the kernel is as in first lemma, a normal subgroup of $Sym(6)$ smaller than $Alt(6)$. Hence kernel is $\{1\}$. Thus one obtains a second isomorphism

$$\pi_2 : Sym(6) \longrightarrow Sym(6) = Sym(Hx_1, Hx_2, \ . \ . \ . \ , Hx_6)$$

Hx_i's are cosets of H in $Sym(6)$.

The correspondence

$$\begin{array}{ccc} Sym(6) & \longrightarrow & Sym(6) \\ \pi_1(\sigma) & \longrightarrow & \pi_2(\sigma) \end{array}$$

is then an automorphism of $Sym(6)$.

$$\pi_1(\sigma\delta) = \pi_1(\sigma)\pi_1(\delta) = \pi_2(\sigma\delta) = \pi_2(\sigma)\pi_2(\delta)$$

This automorphism associates $\langle \pi_1(\sigma) \mid \sigma \in H \rangle$ with $\langle \pi_2(\sigma) \mid \sigma \in H \rangle$.

However, $\langle \pi_2(\sigma) \mid \sigma \in H \rangle$ fixes all the elements in H while $\langle \pi_1(\sigma) | \sigma \in H \rangle$ fixes no elements, indeed if $(Sym(6))_1\tau = Sym(6)_1\tau\sigma$ for all $\sigma \in H$ then $\tau\sigma\tau^{-1} \in Sym(6)_1$ for all $\sigma \in H$, it follows that, $\tau H \tau^{-1} = Sym(6)_1$ which makes $Sym(6)_1$ and H conjugate. Both H and $Sym(6)_1$ are isomorphic to $Sym(5)$ as a subgroup of $Sym(6)$ but they cannot be conjugate since $Sym(6)_1$ is transitive on 5 elements and H on 6 elements. This automorphism of $Sym(6)$ is not inner.

Observe that π_1 and π_2 gives two inequivalent permutation representation of the group $Sym(6)$ but the representations π_1 and π_2 are permutational isomorphic.

5. A

Let F be any field and n any positive integer. Then the set of all invertible $n \times n$ matrices with entries in F form a group with respect to matrix multiplication. This is called **the general linear group of degree** n **over** F and denoted by $GL_n(F)$. Let X be a metric space with distance function $d : X \times X \to \mathbb{R}$. Then a bijective map $\varphi : X \to X$ is structure preserving if $d(x\varphi, y\varphi) = d(x, y)$ for all $x, y \in X$ such a map φ is called **isometry** of X.

5.1. *Assume that a set G with an operation satisfying the associative law satisfies the following two conditions (a) and (b):*

(a) There exists an element e of G such that $ge = g$ for all $g \in G$.

(b) For any element a of G, there exists an element a' such that $aa' = e$.
Then, show that G is a group with respect to the given operation.

Solution We need to show that there exists a left identity and each element has a left inverse. Apply (b) to the element a'. So there exists $a'' \in G$ with $a'a'' = e$. By the associative law;
$ea'' = (aa')a'' = a(a'a'') = ae = a$ by part (a). So we have $ea'' = a$

On the other hand; $ea = (ea)e = (ea)(a'a'') = e(aa')a'' = (ee)a'' = ea'' = a$ by the above paragraph.
Therefore for any element $a \in G$ we have $ea = a = ae$ for all $a \in G$. So, e is the identity element of G.
Since we have $ea'' = a$ and e is the identity element, we get $a'' = a$. So we have $aa' = e$ and $a'a'' = a'a = e = aa'$. So a' is the inverse of a.
Therefore, G is a group with the given conditions.

5.2. *For a given subset X of a group G, let $\mathscr{H}$ be the set of subgroups H satisfying $H \cap X = \emptyset$ (the empty set). The set $\mathscr{H}$ becomes*

a partially ordered set by defining $H \leq K$ if and only if H and K are members of $\mathscr{H}$ and H is a subgroup of K. Show that, if $\mathscr{H}$ is not empty, $\mathscr{H}$ is inductively ordered, so $\mathscr{H}$ has at least one maximal element by Zorn's lemma.
Pick a subgroup H_0 satisfying $H_0 \cap X = \emptyset$, and let $\mathscr{H}_0$ denote the subset of $\mathscr{H}$ consisting of the members which contain H_0. Show that $\mathscr{H}_0$ is also inductively ordered, and has a maximal element.

Solution Assume $\mathscr{H}$ is non-empty. It is clear that $\mathscr{H}$ is a partially ordered set as being a subgroup is a partially ordered set on the set of all subgroups of G. This is the restriction of this relation to $\mathscr{H}$. Since $\mathscr{H} \neq \emptyset$, there exists a subgroup $H_0 \in \mathscr{H}$ such that $H_0 \cap X = \emptyset$. Let

$$\mathscr{H}_0 = \{H \in \mathscr{H} \mid H_0 \leq H \}$$

Let $H_i, i \in I$ be a chain of subgroups in $\mathscr{H}_0$. Then $T = \bigcup_{i \in I} H_i$ is a subgroup of G and $T \in \mathscr{H}_0$ as $T \cap X = \emptyset$. Hence every ascending chain of members in $\mathscr{H}_0$ has an upper bound in $\mathscr{H}_0$. Then by Zorn's lemma there exists a maximal element in $\mathscr{H}_0$. i.e. There exists a subgroup M of G such that M is a maximal element in $\mathscr{H}_0$. Therefore every subgroup containing M will have a non-empty intersection.

5.3.

$$\begin{aligned} \textit{Let } G &= \oplus_{n \in \mathbb{N}^+} \mathbb{Z}_{2^{n+1}} = \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{16} \oplus \cdots \\ H &= \oplus_{n \in \mathbb{N}^+} \mathbb{Z}_{2^n} = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{16} \oplus \cdots \end{aligned}$$

Show that G is not isomorphic to H.

Solution: Observe first that $H = \mathbb{Z}_2 \oplus G$. Then there exists a projection from H to $\mathbb{Z}_2$.

If $G \cong H$, then there exists a projection from G to $\mathbb{Z}_2$. Then

$\pi : G \to \mathbb{Z}_2$ such that $G/ker(\pi) \cong \mathbb{Z}_2$. $\pi^2 = \pi$. By the property of the projection we have $G = \mathbb{Z}_2 \oplus Ker(\pi)$.

Then there exists an epimorphism from finite group

$$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \ldots \oplus \mathbb{Z}_{2^{n+1}} \to \mathbb{Z}_2.$$

Then

$$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \cdots \oplus \mathbb{Z}_{2^{n+1}} \cong \mathbb{Z}_2 \oplus Ker(\pi)$$

$$= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus + \cdots + \mathbb{Z}_{2^n}$$

But this is impossible as direct sums has different maximal elementary abelian subgroups.

5.4. *Let G be the group of 2×2 nonsingular matrices over $\mathbb{R}$. Show that G is a semidirect product of the group of matrices with determinant 1 and the multiplicative group $\mathbb{R}^*$. Describe an action associated with this semidirect product.*
(Hint. The action is not unique. Why not?)

Solution Let $G = GL(2, \mathbb{R})$ Show that $G \cong SL(2, \mathbb{R}) \rtimes \mathbb{R}^*$
Define $\varphi : \mathbb{R}^* \to GL(2, \mathbb{R})$ by $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$. Say $\varphi(\mathbb{R}^*) = H$.
$Ker(\varphi) = 1$, so φ is one-to-one. Then we have $\mathbb{R}^* \cong H \leq GL(2, \mathbb{R})$.
We now show that $SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$
Define $\theta : GL(2, \mathbb{R}) \to \mathbb{R}^*$ by $\theta(A) = det(A)$.
We know that determinant is a homomorphism. Then
$Ker(\theta) = \{A \in GL(2, \mathbb{R}) \mid \theta(A) = det(A) = 1\} = SL(2, \mathbb{R})$
Being the kernel of a homomorphism, we have $SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$.
Now, $H \cap SL(2, \mathbb{R}) = \{A \in H \mid det(A) = 1\} = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$
So we have $G \cong SL(2, \mathbb{R}) \rtimes \mathbb{R}^*$.
Arbitrary element of G can be written as
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad - bc & o \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{a}{ad-bc} & \frac{b}{ad-bc} \\ c & d \end{pmatrix}$ where $\begin{pmatrix} ad - bc & o \\ 0 & 1 \end{pmatrix}$ is in H and $\begin{pmatrix} \frac{a}{ad-bc} & \frac{b}{ad-bc} \\ c & d \end{pmatrix}$ is in $SL(2, \mathbb{R})$

Remark In the above question $G = GL(2, \mathbb{R})$, but the proof will work exactly the same manner for $GL(n, \mathbb{R})$ or $GL(n, \mathbb{F})$.

One may take $K = \begin{pmatrix} 1 & 0 \\ 0 & ad - bc \end{pmatrix}$. Then $K \cong \mathbb{R}^*$ then the homomorphism and the action is not the same.

5.5. *Find the number of left cosets of K which are contained in the double coset HxK, also show that G is the disjoint union of its (H,K)-double cosets.*

Solution

5.6. *Let H be a proper subgroup of a finite group G. Show that there exists an element of G which is not conjugate to any element of H.*

Solution Assume for any $x \in G$, there exists $g \in G$ such that $x \in H^g$. Then $G = \bigcup H^g$. Let $|G| = n$ and $|H| = k$.
The number of distinct conjugates of H is $[G : N_G(H)]$.

Then we have $|G| = [G : N_G(H)]|N_G(H)| \geq [G : N_G(H)]|H|$ as $N_G(H) \geq H$. Let $|G : N_G(H)| = m$. Then H has m distinct conjugates in G. Say $H = H^1, H^{g_2}, \ldots, H^{g_m}$. As each H^{g_i} contain $|H| - 1$ non-identity element we have at most $|H^{g_i}| - 1$ non-identity element in H^{g_i}. If $G = \bigcup_{i=1}^{m} H^{g_i}$. Then $|G| = \sum_{i=1}^{m}(|(H^{g_i} - id)| \leq (k-1)m + 1$ as $H \leq N_G(H)$ we have $mk - m + 1 \geq |G| = m(|N_G(H)| \geq mk$. So we have $-m + 1 \geq 0$ and $m \leq 1$. But $m = 1$ implies that $H \lhd G$ and in this case $H^g = H$ for all $g \in G$. This implies that $H = G$. This contradicts to the assumption that H is a proper subgroup of G. So G cannot be a union of conjugates of a proper subgroup H.

5.7. *For any proper subgroup H of a group G, $HH^x \neq G$ for any $x \in G$.*

Solution Assume that $HH^x = G$ for some $x \in G$. Since H is a proper subgroup, clearly $x \neq 1$. Then $x = h_1 h_2^x$ for some $h_1, h_2 \in H$. Then $x = h_1 x^{-1} h_2 x$. It follows that $1 = h_1 x^{-1} h_2$ and so $h_1^{-1} h_2^{-1} = x^{-1}$. Since H is a subgroup and $h_1, h_2 \in H$ we have $h_1^{-1} h_2^{-1} \in H$ i.e. $x \in H$. But then, $G = HH^x = H$. This contradicts to H is a proper subgroup. Hence $HH^x \neq G$.

5.8. ***(a)*** *Prove that any subgroup of index 2 is normal.*
(b) *Let G be a finite group, and let p be the smallest prime divisor of the order $|G|$. Show that any subgroup of index p is normal.*

Solution (a) Let $H \leq G$ with $[G : H] = 2$.
Then H has two distinct right cosets, and also two distinct left cosets in G. For any $h \in H$, we have $hH = Hh = H$ and for any $a \in G$ with $a \notin H$, we have $aH \neq H$ and $Ha \neq H$. Since there are exactly two cosets of H in G, we have $Ha = aH = G \setminus H$ for all $a \in G$.
Therefore $H \trianglelefteq G$.

(b) Let H be a subgroup of G of index p. Then we need to show that H is a normal subgroup of G. Indeed G acts from right on the set of right cosets of H in G. Then there exists a homomorphism from G into $Sym(p)$. Then $G/Ker(\phi)$ is isomorphic to a subgroup of $Sym(p)$. Recall that $Ker(\phi) = \bigcap_{x \in G} H^x$. So $Ker(\phi) \leq H$. If H is not normal in G, then $Ker(\phi)$ will be a proper subgroup of H and hence $1 \neq H/Ker(\phi) < G/Ker(\phi)$. i.e a prime divisor of $|H/Ker(\phi)|$ divides $|G|/|Ker(\phi)|$ which divides $\frac{p!}{|Ker(\phi)|}$. Hence it divides $|G|$ which is impossible as any prime dividing $p!$ is less than p and p is the smallest prime dividing $|G|$.

Definition 5.1. *An endomorphism σ of a group G is said to be normal if σ commutes with all inner automorphisms of G.*

5.9. *Let σ be a normal endomorphism of a group G. Set $\sigma(G) = H$ and $\sigma(g) = z(g)^{-1}g$ for any $g \in G$.*

(a) *Show that z is a homomorphism from G into $C_G(H)$.*

(b) *Show that H is a normal subgroup of G such that $G = HC_G(H)$, and $H \cap C_G(H) = Z(H) \subset Z(G)$.*

(c) *Show that both H and $C_G(H)$ are invariant by σ. Prove that the restriction ρ of σ on $C_G(H)$ is a homomorphism from $C_G(H)$ into $Z(H)$, and that for any element x of $Z(H)$, we have $x = \zeta(x)\rho(x)$ where ζ is the restriction of z on H.*

Solution

(a) Let σ be a normal endomorphism of a group G. Then σ is an endomorphism of G, commuting with all the inner automorphisms of G. Let $\sigma(G) = H$ and $\sigma(g) = z(g)^{-1}g$. We may view this as $z(g) = g\sigma(g)^{-1}$.

First observe that $z(g) = g\sigma(g)^{-1} \in C_G(H)$. Indeed;

$i_g\sigma = \sigma i_g$ implies for any $x \in G$ $((x)i_g)\sigma = ((x)\sigma)i_g$. Then $(g^{-1}xg)\sigma = g^{-1}((x)\sigma)g$. It follows that

$((g^{-1})\sigma)((x)\sigma)((g)\sigma) = g^{-1}((x)\sigma)g$. Multiply from left by g and from right by g^{-1} we have $[g((g^{-1})\sigma)]((x)\sigma)(g)\sigma)g^{-1} = (x)\sigma$ for any $x \in G$. So for any $(x)\sigma \in H$ we have $z(g) = g(g^{-1})\sigma \in C_G(H)$.

Now for any g and h in G we have;

$(gh)z = gh((gh)\sigma)^{-1} = gh((g)\sigma(h)\sigma)^{-1} = gh((h)\sigma)^{-1}((g)\sigma)^{-1}$

By first paragraph $h(h^{-1})\sigma \in C_G(H)$ so $h(h^{-1})\sigma$ commutes with $(g^{-1})\sigma$ and we obtain

$(gh)z = g((g^{-1})\sigma)h((h^{-1})\sigma) = (g)z(h)z$. Hence z is a homomorphism from G into $C_G(H)$.

(b) $H = (G)\sigma$. For any $g \in G$ and $(x)\sigma \in H$

$g^{-1}(x)\sigma g = g^{-1}(x)\sigma g((g)\sigma)^{-1}(g)\sigma$ as $g((g)\sigma)^{-1} \in C_G(H)$ we have

$= g^{-1}g((g)\sigma)^{-1}(x)\sigma(g)\sigma = ((g)\sigma)^{-1}(x)\sigma(g)\sigma = (g^{-1}xg)\sigma \in H$.

So H is a normal subgroup of G.

Now for any $g \in G$

$g = (g)\sigma g((g)\sigma)^{-1}$ as $g((g)\sigma)^{-1} \in C_G(H)$ and $(g)\sigma \in H$ we have

$G = HC_G(H)$ and $H \cap C_G(H) = Z(H)$.

Indeed if $x \in H \cap C_G(H)$, then for any $g \in G$

$gx = (g)\sigma g((g^{-1})\sigma)x$

$= (g)\sigma x g((g^{-1})\sigma)$ as $x \in H$ and $g((g^{-1})\sigma) \in C_G(H)$

$= x(g)\sigma g((g^{-1})\sigma)$ as $x \in C_G(H)$ and $(g)\sigma \in H$.

$= xg$.

So $x \in Z(G)$ and hence $Z(H) = H \cap C_G(H) \leq Z(G)$.

(c)(i) H is invariant as $(H)\sigma = ((G)\sigma)\sigma \subseteq (G)\sigma = H$

Let $x \in C_G(H)$. Then for any $h \in H, xh = hx$.

i.e. $x(g)\sigma = (g)\sigma x$ for any $g \in G$. Then $x(g)\sigma x^{-1} = (g)\sigma$ for all $g \in G$.

Now we consider the following $(x)\sigma(g)\sigma = (g)\sigma(x)\sigma$?

$(x)\sigma x^{-1}x(g)\sigma = (x)\sigma x^{-1}(g)\sigma x$

$= (g)\sigma(x)\sigma x^{-1}x$ as $(x)\sigma x^{-1} = (x(x^{-1})\sigma)^{-1} \in C_G(H)$ and $(g)\sigma \in H$

$= (g)\sigma(x)\sigma$

Hence $(x)\sigma \in C_G(H)$.

(ii) The restriction ρ:

Let $x, y \in C_G(H)$. Then $(x)\rho = (x)\sigma = ((x)z)^{-1}x$. $((x)z)^{-1}x \in Z(H)$ as for any $(g)\sigma \in H$, we have $((x)z)^{-1}x(g)\sigma = ((x)z)^{-1}(g)\sigma x$ as $x \in C_G(H)$ and $(g)\sigma \in H$. Now as $(x)z \in C_G(H)$ we have $((x)z)^{-1}x(g)\sigma = (g)\sigma((x)z)^{-1}x$. It follows that $((x)z)^{-1}x \in Z(H)$ and $(x)\rho \in Z(H)$.

Moreover $(xy)\rho = (xy)\sigma = (x)\sigma(y)\sigma = (x)\rho(y)\rho$

(iii) Let $x \in Z(H)$. Then $x = x((x)\sigma)^{-1}(x)\sigma$.

Now $x((x)\sigma)^{-1} = (x)z = (x)\zeta$ where ζ is the restriction of z on H. And $(x)\sigma = (x)\rho$ where ρ is the restriction of σ on $C_G(H)$.

5.10. *Let G be a group with $Z(G)$=1. Show that the centralizer in $Aut(G)$ of $Inn(G)$ is $\{1\}$ and in particular, $Z(Aut(G))$=$\{1\}$.*

Solution: Let $\phi \in C_{Aut(G)}(Inn(G))$. Then

$\phi^{-1}i_g\phi = i_g$ for any $i_g \in Inn(G)$. For any element $x \in G$, $\phi^{-1}i_g\phi(x) = i_g(x)$ and so $\phi^{-1}i_g(\phi(x)) = g^{-1}xg$. It follows that $\phi^{-1}(g^{-1}\phi(x)g) = g^{-1}xg$ iff $\phi^{-1}(g^{-1})x\phi^{-1}(g) = g^{-1}xg$. Then we have

$g\phi^{-1}(g^{-1})x\phi^{-1}(g)g^{-1} = x$. Hence

$(g^{-1})^{-1}(\phi^{-1}(g))^{-1}x\phi^{-1}(g)g^{-1} = x$ for all $x \in G$.

Hence, $\phi^{-1}(g)g^{-1} \in Z(G) = \{1\}$. It follows that $\phi^{-1}(g) = g$ for all $g \in G$. Then the automorphism ϕ^{-1} fixes all the elements of G. i.e. ϕ^{-1} and hence ϕ is the identity automorphism of G.

As $Z(Aut(G)) = C_{Aut(G)}(Aut(G)) \leq C_{Aut(G)}(Inn(G)) = \{1\}$, we have $Z(Aut(G)) = \{1\}$. It follows that $Z(G) = \{1\}$ implies $Z(Aut(G)) = \{1\}$.

5.11. *Let G be a nonabelian simple group. Show that any automorphism of $Aut(G)$ is inner.*

Solution: As G is nonabelian simple group, $Z(G)$=$\{1\}$. Then by Question 5.10, $Z(Aut(G)) = \{1\}$. Then by Question **??**, any automorphism of $A = Aut(G)$ is an inner automorphism.

5.12. *If two subgroups H and K of a group G satisfy the conditions $H \cap K = \{1\}$, $H \leq N_G(K)$ and $K \leq N_G(H)$, then every element of H commutes with every element of K.*

Solution: Consider the element $h^{-1}k^{-1}hk$. Since $K \leq N_G(H)$, $k^{-1}hk \in H$. So $h^{-1}k^{-1}hk \in H$. Similarly, $H \leq N_G(K)$ implies $k^{-1}hk \in K$. So $h^{-1}k^{-1}hk \in K$. Hence, $h^{-1}k^{-1}hk \in H \cap K = \{1\}$. It follows that $h^{-1}k^{-1}hk = 1$ and so $hk = kh$ for any $h \in H$ and $k \in K$.

5.13. *Let G be a group with a composition series and let N be a normal subgroup of G. Show that there is a composition series of G having N as a term.*

Solution: Let G be a group with a composition series $G = G_0 \triangleright G_1 \triangleright .. \triangleright G_n = \{1\}$.

Take the intersection of each subgroup in the series with the normal subgroup N. We have $G_0 \cap N = N \triangleright G_1 \cap N \triangleright G_2 \cap N \triangleright .. \triangleright G_n \cap N = \{1\}$.

Now, we need to show $G_{i+1} \cap N \trianglelefteq G_i \cap N$. Indeed, let $x \in G_{i+1} \cap N$ and $g \in G_i \cap N$. Then $g^{-1}xg \in N$ as $x \in N$ an N is a normal subgroup of G. Moreover, $x \in G_{i+1}$ and $g \in G_i$ and G_{i+1} is normal in G_i implies $g^{-1}xg \in G_{i+1}$. Hence, $x \in G_{i+1} \cap N$ and so $G_{i+1} \cap N \trianglelefteq G_i \cap N$.

$(G_i \cap N)/(G_{i+1} \cap N) \simeq (G_i \cap N)G_{i+1}/G_{i+1} \trianglelefteq G_i/G_{i+1}$.

But G_i/G_{i+1} is a composition factor of the group G. So $(G_i \cap N)/(G_{i+1} \cap N)$ is either equal to G_i/G_{i+1} or $\{1\}$.

So it is simple or $(G_i \cap N)G_{i+1}/G_{i+1}$ is the trivial group.

So N has a series where each factor is either simple and the simple factor is isomorphic to a simple factor of G or it is trivial group. By deleting the trivial terms from the series, we obtain a composition series of N.

Now we may look at the series $G \triangleright G_1N \triangleleft G_2N \dots N$ this series also give a series from G to N with factors are either trivial or simple apply the same procedure above and obtain a series of G where N is a term of this series.

5.14. *Show that the following two conditions on a group G are equivalent:*

(1) There is a homomorphism φ from G into $Sym(n)$ such that $\varphi(g) \neq 1$ for some $g \in G$.

(2) The group G contains a proper subgroup of index at most n.

Solution (a) $\Rightarrow$ (b): Assume that there is a homomorphism $\varphi : G \to Sym(n)$ such that $\varphi(g) \neq 1$ for some $g \in G$.

Let G act on the set $X = \{1, 2, .., n\}$. As

$$Ker(\varphi) = \{g \in G \mid \varphi(g) = 1\}$$

and $\varphi(g) \neq 1$ for some $g \in G$, the action of G on X is no-trivial.

Let $x \in X$ such that $x^g \neq x >$ for some $g \in G$. Then $O_x \neq \{x\}$. This implies that $|O_x| > 1$.

By Orbit-Stabilizer Theorem, $|G : Stab_G(x)| = |O_x| \leq n$. This implies that $Stab_G(x)$ is a proper subgroup of G as $|O_x| > 1$ and the index of $Stab_G(x)$ is at most n.

(b) $\Rightarrow$ (a): Assume that H is a proper subgroup of G of index at most n, say $[G : H] = k$. Let Ω be the set of right cosets of H in G. Then G act on Ω by right multiplication. Observe that $|\Omega| = k$.

As G act on Ω, there exists a homomorphism $\varphi : G \to Sym(k)$ by $\varphi(g)Hx = Hxg$.

As $Ker(\varphi)$ contains all elements $g \in G$ such that $g \in \bigcap_{x \in G} H^x$ we have $Ker(\varphi) \leq H$. Hence, for any $g \in G \setminus H$ we have $\varphi(g) \neq 1$.

References

[1] D. J. S. Robinson, A course in Group Theory, GTM 80, Springer-Verlag.