Suns

Eric Liu

Contents

Chapter 1

Groups

1.1 Group action

Let M be a set equipped with a binary operation $M \times M \to M$. We say M is a **monoid** if the binary operation is associative and there exists a two-sided identity $e \in M$.

Example 1.1.1

Defining $(x, y) \mapsto y$, we see that the operation is associative and every element is a left identity, but no element is a right identity unless $|M| = 1$. This is an example why identity must be two-sided.

Because the identity of a monoid is defined to be two-sided, clearly it must be unique. Suppose every element of monoid M has a left inverse. Fix $x \in M$. Let $x^{-1} \in M$ be a left inverse of x. To see that x^{-1} is also a right inverse of x, let $(x^{-1})^{-1} \in M$ be a left inverse of x^{-1} and use

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x$$

to deduce

$$xx^{-1} = (x^{-1})^{-1}x^{-1} = e$$

In other words, if we require every element of a monoid M to has a left inverse, then immediately every left inverse upgrades to a right inverse. In such case, we call M a **group**. Notice that inverses of elements of a group are clearly unique.

Example 1.1.2

Another set of axioms for group is to require the operation to be associative, identity to be left, and the existence of left inverses. Under such condition, we see that if an element y is **idempotent**, then it must be identity, since $y = (y^{-1}y)y = y^{-1}y = e$. Because of such, we see a left inverse is also a right inverse, since $(xx^{-1})(xx^{-1}) = xex^{-1} = xx^{-1}$. This then shows that the left identity is also a right identity, since $xe = x(x^{-1}x) = x$.

Example 1.1.3

If the underlying set is finite, then weaker assumption can be made. For example, suppose only that the binary operation to be associative and that both cancellation holds:

$$au = aw \implies u = w \quad \text{and} \quad ua = wa \implies u = w$$

Because the set is finite, for all a, we may attach it with an natural number $n(a)$ such that $a^{n(a)+1} = a$. Clearly,

$$aa^{n(a)}b = a^{n(a)+1}b = ab = ab^{n(b)+1} = ab^{n(b)}b$$

This then by cancellation laws implies $a^{n(a)} = b^{n(b)}$, which can be easily checked to be the identity.

Example 1.1.4

By example 1.1.3, we see that the set of nonzero integer relatively prime to n and modulo n forms a group under multiplication modulo n, called the **multiplicative group of integer modulo** n, or equivalently the unit group of the ring $\mathbb{Z}_n$.

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \to H$, if φ respects the binary operation, then φ also respects the identity:

$$e_H = (\varphi(x)^{-1})\varphi(x) = (\varphi(x)^{-1})\varphi(xe_G) = (\varphi(x)^{-1}\varphi(x))\varphi(e_G) = \varphi(e_G)$$

which implies that φ must also respect inverse. In such case, we call φ a **group homomorphism**. In this note, by a **subgroup** H of G, we mean an injective group homomorphism $H \hookrightarrow G$. Clearly, a subset of G forms a subgroup if and only if it is closed under both the binary operation and inverse. Note that one of the key basic property of subgroup $H \subseteq G$ is that if $g \notin H$, then $hg \notin H$, since otherwise $g = h^{-1}hg \in H$.

Let S be a subset of G. The group of **words** in S:

$$\{s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in G : n \in \mathbb{N} \cup \{0\} \text{ and } s_i \in S \text{ and } \epsilon_i = \pm 1\}$$

is clearly the smallest subgroup of G containing S. We say this subgroup is **generated** by S. If G is generated by a single element, we say G is **cyclic**. Let $x \in G$. The **order** of G is the cardinality of G, and the order of x is the cardinality of the cyclic subgroup $\langle x \rangle \subseteq G$, or equivalently the infimum of the set of natural numbers n that makes $x^n = e$. Clearly, finite cyclic groups of order n are all isomorphic to $\mathbb{Z}_n$.

Let G be a group and H a subgroup of G. The **right cosets** Hx are defined by $Hx \triangleq \{hx \in G : h \in H\}$. Clearly, when we define an equivalence relation in G by setting:

$$x \sim y \overset{\triangle}{\iff} xy^{-1} \in H$$

the equivalence class $[x]$ coincides with the right coset Hx. Note that if we partition G using **left cosets**, the equivalence relation being $x \sim y \iff x^{-1}y \in H$, then the two partitions need not to be identical.

Example 1.1.5. Let $H \triangleq \{e, (1,2)\} \subseteq S_3$. The right cosets are

$$H(2,3) = \{(2,3), (1,2,3)\} \quad \text{and} \quad H(1,3) = \{(1,3), (1,3,2)\}$$

while the left cosets being

$$(2,3)H = \{(2,3), (1,3,2)\} \quad \text{and} \quad (1,3)H = \{(1,3), (1,2,3)\}$$

■

However, as one may verify, we have a well-defined bijection $xH \mapsto Hx^{-1}$ between the sets of left cosets and right cosets of H. Therefore, we may define the **index** $[G : H]$ of H in G to be the cardinality of the collection of left cosets of H, without falling into the discussion of left and right. Moreover, let K be a subgroup of H, by axiom of choice, clearly we have:

$$[G : K] = [G : H] \cdot [H : K]$$

which gives **Lagrange's theorem**

$$o(G) = [G : H] \cdot o(H)$$

as a corollary.

Let G be a group and X a set. If we say G **acts on X from left** we are defining a function $G \times X \to X$ such that

(i) $e \cdot x = x$ for all $x \in X$.

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

Note that there is a difference between left action and right action, as gh means $g \circ h$ in left action and means $h \circ g$ in right action.
Because groups admit inverses, a G-action is in fact a group homomorphism $G \to \text{Sym}(X)$. The trivial action then correspond to the trivial group homomorphism. An action is **faithful** if it is injective.

Show that $Z(G) \subseteq \operatorname{Ker} \theta$ if and only if θ is faithful.

An action is **free** if $g \cdot x = x$ for a $x \in X$ implies $g = e$. Note that the isomorphism $\text{Sym}(X) \to \text{Sym}(X)$ is always injective but never free unless $|X| \leq 2$. The action is **transitive** if for any $x, y \in X$, there always exists some $g \in G$ such that $y = g \cdot x$. An action is **regular** if it is both free and transitive.

Let $x \in X$. We call the set $G \cdot x \triangleq \{g \cdot x \in X : g \in G\}$ the **orbit** of x. Clearly the set G_x of all elements of G that fixes x forms a group, called the **stabilizer subgroup** of G with respect to x. Consider the action left. The fact that the obvious mapping between the set of left cosets of stabilizer subgroups of G with respect to x to the orbit of x:

$$\{gG_x \subseteq G : g \in G\} \longleftrightarrow G \cdot x$$

forms a bijection is called the **orbit-stabilizer theorem**, which relates the index of the stabilizer subgroup of x and the orbit of x:

$$[G : G_x] = |G \cdot x|$$

Example 1.1.6. Let H be a subgroup of G, and let H acts on G by right multiplication. Then the orbit of $x \in G$ is just the left coset xH, while the stabilizer subgroup H_x is trivial, agreeing with orbit-stabilizer theorem.

Theorem 1.1.7. (Cauchy's theorem for finite group) Let $p \mid o(G)$. Then the number of elements of order divided by p is a positive multiple of p.

Proof. The set X of p-tuples $(x_1, \dots, x_p)$ that satisfies $x_1 \cdots x_p = e$ clearly has cardinality $o(G)^{p-1}$. Consider the group action $\mathbb{Z}_p \to \text{Sym}(X)$ defined by

$$g \cdot (x_1, \dots, x_p) \triangleq (x_p, x_1, \dots, x_{p-1}), \qquad \text{where } \mathbb{Z}_p = \langle g \rangle$$

Notice that $x^p = e$ if and only if $(x, \dots, x) \in X$. Therefore the number of cardinality 1 orbit equals to number of solution to $x^p = e$. By orbit-stabilizer theorem, an orbit in X either has cardinality p or 1. Therefore, we may write

$$p \mid o(G)^{p-1} = m + kp$$

with m the number of cardinality 1 orbits and k the number of cardinality p orbits. Clearly we have $p \mid m$, as desired. ■

1.2 Normalizer and centralizer

Because the inverse of an injective group homomorphism forms a group homomorphism, we know the set $\text{Aut}(G)$ of automorphisms of G forms a group. We say $\phi \in \text{Aut}(G)$ is an **inner automorphism** if ϕ takes the form $x \mapsto gxg^{-1}$ for some fixed $g \in G$. We say two elements $x, y \in G$ are **conjugated** if there exists some inner automorphism that maps x to y. Clearly conjugacy forms a equivalence relation. We call its classes **conjugacy classes**.

Equivalent Definition 1.2.1. (Normalize)

From the point of view of inner automorphism, we see that it is well-defined whether an element $g \in G$ **normalize** a subset $S \subseteq G$:

$$\left\{gsg^{-1} \in G : s \in S\right\} = S$$

independent of left and right. Because of the independence, For each subset $S \subseteq G$, we see that the set of elements $g \in G$ that normalize S forms a group, called the **normalizer** of S. Note that if g normalize S, then $gS = Sg$.

Example 1.2.2. Consider $G \triangleq \text{GL}_2(\mathbb{R})$ and consider:

$$H \triangleq \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) : n \in \mathbb{Z}\right\} \quad \text{and} \quad g \triangleq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$$

Note that $gHg^{-1} \subset H$. In other words, inner automorphisms can maps a subgroup H into a subgroup strictly contained by H if G is infinite.

Equivalent Definition 1.2.3. (Normal subgroups) Let G be a group and N a subgroup. We say N is a **normal subgroup** of G if any of the followings hold true:

(i) $\phi(N) \subseteq N$ for all $\phi \in \text{Inn}(G)$

(ii) $\phi(N) = N$ for all $\phi \in \text{Inn}(G)$

(iii) $xN = Nx$ for all $x \in G$.

(iv) The set of all left cosets of N equals the set of all right cosets of N.

(v) N is a union of conjugacy classes.

(vi) For all $n \in N$ and $x \in G$, their **commutator** $nxn^{-1}x^{-1} \in G$ lies in N.

(vii) For all $x, y \in G$, we have $xy \in N \iff yx \in N$.

Proof. (i) $\implies$ (ii): Let $\phi \in \text{Inn}(G)$. By premise, $\phi(N) \subseteq N$ and $\phi^{-1}(N) \subseteq N$. Applying ϕ to both side of $\phi^{-1}(N) \subseteq N$, we have $\phi(N) \subseteq N \subseteq \phi(N)$, as desired.

(ii) $\implies$ (iii): Consider the automorphisms:

$$\phi_{L,x}(g) = xg \quad \text{and} \quad \phi_{L,x^{-1}}(g) = x^{-1}g \quad \text{and} \quad \phi_{R,x}(g) = gx$$

Because $\phi_{L,x^{-1}} \circ \phi_{R,x} \in \text{Inn}(G)$, by premise we have:

$$xN = \phi_{L,x}(N) = \phi_{L,x} \circ \phi_{L,x^{-1}} \circ \phi_{R,x}(N) = \phi_{R,x}(N) = Nx$$

(iii) $\implies$ (iv) is clear. (iv) $\implies$ (iii): Let $x \in G$. By premise, there exists some $y \in G$ that makes $xN = Ny$. Let $x = ny$. The proof then follows from noting

$$xN = Ny = N(n^{-1}x) = Nx$$

(iii) $\implies$ (v): Let $n \in N$ and $x \in G$. We are required to show $xnx^{-1} \in N$. Because $xN = NX$, we know $xn = \widetilde{n}x$ for some $\widetilde{n} \in N$. This implies

$$xnx^{-1} = \widetilde{n}xx^{-1} = \widetilde{n} \in N$$

(v) $\implies$ (vi): Fix $n \in N$ and $x \in G$. By premise, $xn^{-1}x^{-1} \in N$. Therefore, $n(xn^{-1}x^{-1}) \in N$, as desired.

(vi) $\implies$ (vii): Let $xy \in N$. To see yx also belong to N, observe:

$$(xy)^{-1}(yx) = (xy)^{-1}x^{-1}xyx = [xy, x] \in N$$

(viii) $\implies$ (i): Let $n \in N$ and $x \in G$. Because $(nx)x^{-1} = n \in N$, by premise we have $x^{-1}nx \in N$, as desired. ■

Equivalent Definition 1.2.4. (Normal closure) Let G be a group and $S \subseteq G$. The **normal closure** $\text{ncl}_G(S)$ of S in G refer to any one of the followings:

(i) The smallest normal subgroup of G containing S, which we know exists as the intersection of all normal subgroups of G containing S.

(ii) The subgroup of G generated by

$$\bigcup_{\phi \in \text{Inn}(G)} \{\phi(x) \in G : x \in S\}$$

Proof. We are required to prove the subgroup of G from (ii) is normal. Clearly, it is the set:

$$\left\{g_1^{-1}x_1^{\epsilon_1}g_1 \cdots g_n^{-1}x_n^{\epsilon_n}g_n \in G : n \geq 0, x_i \in S, \epsilon_i = \pm 1, g_i \in G\right\}$$

Fix $g \in G$. The proof then follows from noting

$$g^{-1}\left(g_1^{-1}x_1^{\epsilon_1}g_1 \cdots g_n^{-1}x_n^{\epsilon_n}g_n\right)g = \Big(\left(g_1g\right)^{-1}x_1^{\epsilon_1}\left(g_1g\right)\Big)\cdots\Big(\left(g_ng\right)^{-1}x_n^{\epsilon_n}\left(g_ng\right)\Big)$$

$\blacksquare$

We denote the **centralizer** $C_G(S) \triangleq \big\{g \in G : gsg^{-1} = s \text{ for all } s \in S\big\}$. We call the centralizer of the whole group $Z(G) \triangleq C_G(G)$ **center**. Clearly $Z(G)$ forms an abelian subgroup of G, and every element of the center form a single conjugacy classes.

For finite group G, we have the **class equation**

$$|G| = |Z(G)| + \sum |G : C_G(x)|$$

where x runs through conjugacy classes outside of $Z(G)$.

Clearly $C_G(S) \subseteq N_G(S)$.

1.3 Isomorphism theorems

Let G be a group and $N \subseteq G$ a normal subgroup. We say a group homomorphism $\pi : G \to G/N$ satisfies the **universal property of quotient group G/N** if

(i) it vanishes on N. **(Group condition)**

(ii) for all group homomorphism $f : G \to H$ that vanishes on N there exist a unique group homomorphism $\widetilde{f} : G/N \to H$ that makes the diagram:

$$\begin{tikzcd}
G \arrow[r, two heads, "\pi"] \arrow[dr, "f"'] & G/N \arrow[d, "\widetilde{f}"] \\
& H
\end{tikzcd}$$

commute. **(Universality)**

Theorem 1.3.1. (The first isomorphism theorem for groups) The group homomorphism $\pi : G \to G/N$ is always surjective with kernel N. Let $f : G \to H$ be a group homomorphism. Then $\ker f$ is normal in G, and the induced homomorphism $\widetilde{f} : G/\ker f \to H$ is injective.

Proof. The first part is an immediate consequence of construction of G/N. However, it should be noted that such construction can be avoided. The fact that $\ker(\pi) = N$ can be proved by considering the permutation representation $G \to \text{Sym}(\Omega)$, where Ω is the set of the cosets of N, and the fact that π is surjective is a consequence of $\widetilde{\pi} = \mathbf{id}_{G/N}$.

We clearly have $\ker f \trianglelefteq G$. The fact that $\widetilde{f} : G/\ker f \to H$ is injective follows from $\pi : G \to G/\ker f$ being surjective with kernel $\ker f$. ■

Because the kernel of a group homomorphism is clearly normal, if N is not normal, then there can not be a pair $G \to G/N$ that satisfies the universal property. If any things, this is the "reason" why normal subgroups are what meant to be quotiented in the category of group.

Given $x, y \in G$, we often write

$$[x, y] \triangleq xyx^{-1}y^{-1} \quad \text{or} \quad [x, y] \triangleq x^{-1}y^{-1}xy$$

and call $[x, y]$ the **commutator** of x and y. Independent of differences of the definition, we have $[x, y] \in N$ if and only if $xyN = yxN$. Again, independent of the definition, the

commutator subgroup $[G,G]$ of G is the subgroup generated by the commutators. It should be noted that given a normal subgroup N of G, the quotient group G/N is abelian if and only if N contains the commutator subgroup of G.

Example 1.3.2. $G \triangleq S_3$. $S \triangleq \langle (1,2) \rangle$ and $H \triangleq \langle (2,3) \rangle$. SH doesn't form a group. $(2,3)(1,2) \notin SH$.

Theorem 1.3.3. (Second isomorphism theorem) Let $H \leq G$. If K is a subgroup of normalizer of H, then their product:

$$HK \triangleq \{hk \in G : h \in H \text{ and } k \in K\}$$

forms a group (in fact, the subgroup generated by $H \cup K$) and is defined independent of left and right. Moreover, $H \trianglelefteq HK$ with $hkH = Hk$, and $H \cap K \trianglelefteq K$ with

$$HK/H \cong K/H \cap K \quad \text{via} \quad kH \longleftrightarrow k(H \cap K)$$

Proof. ■

Third isomorphism theorem.
Correspondence theorem.
Because $\varphi \circ \phi_g \circ \varphi^{-1} = \phi_{\varphi(g)}$, we know $\text{Inn}(G)$ forms a normal subgroup of $\text{Aut}(G)$.

1.4 Sylow theorems

Theorem 1.4.1. (First and Third Sylow theorem, Wielandt's proofs) Let G be a finite group of order $p^m t$ with $\gcd(p,t)=1$. Let $r \leq m$. Then the number n_p of p-subgroup with order p^r satisfies

$$n_p \equiv 1 \pmod p$$

Proof. Let X be the set of subset of G with cardinality p^r. Our goal is to find all elements of X that forms a group. Clearly we may define a left G-action on X be setting

$$g \cdot \{x_1, \dots, x_{p^r}\} \triangleq \{gx_1, \dots, gx_{p^r}\}$$

Let Γ be an orbit. If Γ contains a group, then we see that Γ is the left coset space of that group, containing exactly one group and satisfying $|\Gamma| = p^{m-r}t$. If Γ doesn't contain any group, there still exists some $S \in \Gamma$ such that $e \in S$, and clearly we will have $\text{Stab}(S) \subseteq S$. Because S isn't a group, we see $p^r = |S| > o(\text{Stab}(S))$, which by orbit-stabilizer theorem implies that $|\Gamma| = [G : \text{Stab}(S)] = p^{m-r+c}t$ for some $c \geq 1$.

In summary, by counting orbit, we have shown that:

$$\binom{p^m t}{p^r} = |X| = n_p p^{m-r}t + l p^{m-r+1}t, \qquad \text{for some } l \in \mathbb{N}$$

Let $ut \equiv 1 \pmod p$. Recalling that $\binom{p^m t}{p^r}$ has p-power p^{m-r}, it remains to show

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} \equiv 1 \pmod p$$

which follows from noting:

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} = ut \cdot \binom{p^m t - 1}{p^r - 1} \equiv \binom{p^m t - 1}{p^r - 1} \equiv 1 \pmod p$$

where the last equality follows from Lucas modulo binomial formula. ■

Theorem 1.4.2. (Counting lemma for p-group) Let H be a p-group acting on a finite set Ω. Let Ω_0 be the set of fixed points. Then

$$|\Omega| \equiv |\Omega_0| \pmod p$$

Proof. This is a consequence of orbit-stabilizer theorem. ■

Theorem 1.4.3. (Second Sylow theorem) Sylow p-subgroups are conjugated to each other.

Proof. Let H and P be two Sylow p-subgroups of G, and let H acts on left coset space of P by left multiplication. Because P is Sylow, by counting lemma for p-group, we know the number of fixed points gP is nonzero. Let gP be a fixed point. We then see that, as desired, $g^{-1}hg \in P$ for all $h \in H$, since $hgP = gP$. ■

Theorem 1.4.4. (Remaining part of third Sylow theorem) Let G be a finite group, and let n_p be the number of Sylow p-subgroup of G. For all Sylow p-subgroup P of G, we have

$$n_p = [G : N(P)]$$

Proof. This is a consequence of second Sylow theorem and orbit stabilizer theorem, where we note that when G acts on $\mathrm{Syl}_p(G)$ by conjugation we have $\mathrm{Stab}(P) = N(P)$. ■

Example 1.4.5. Let $o(G) = pq$ with $p > q$ being prime. Because $n_p \equiv 1 \pmod{p}$ and $n_p \mid o(G) = pq$, we see $n_p = 1$.

If

If G is non-abelian, then we must have $q \mid p - 1$, since otherwise

1.5 Finitely generated abelian group

Equivalent Definition 1.5.1. (Internal direct products for groups) Let G be a group with normal subgroups $N_1, \dots, N_k$. We say G is an **internal direct products of** N_i if any of the followings hold true:

(i) The natural map $N_1 \times \cdots \times N_k \to G$ forms a group isomorphism.

(ii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j \neq i} N_j = \{e\}$ for all i.

(iii) Every $g \in G$ can be written uniquely as $\prod n_i$.

Proof. (i) $\implies$ (ii): Clearly we have $N_1 \cdots N_k = G$. Let $n_2 \cdots n_k \in N_1$. Because $n_2 \cdots n_k$ is both the image of $(n_2 \cdots n_k, e, \dots, e)$ and $(e, n_2, \dots, n_k)$, by injectivity of the natural map, we know $n_2 = \cdots = n_k = e$.

(ii) $\implies$ (iii): The existence is clear. To see the uniqueness, observe that $\prod n_i = \prod \widetilde{n}_i$ implies $(\widetilde{n}_1)^{-1} n_1 n_2 \cdots n_k = \widetilde{n}_2 \cdots \widetilde{n}_k$

■

Example 1.5.2. Let $G \triangleq \mathbb{Z}_4 \times \mathbb{Z}_2$. Clearly the direct product of $\langle (1,0) \rangle$ and $\langle (2,0) \rangle$ is isomorphic to G, but they do not form an internal direct product of G. It is because of such, we must require $N_1 \times \cdots \times N_k$ not only isomorphic to G, but moreover the natural way in definition of internal direct products for groups.

Theorem 1.5.3. (Fundamental theorem for finite abelian group)

Theorem 1.5.4. (Fundamental theorem for finitely generated abelian group)

1.6 Nilpotency and Solvability

More than often, we care about the existence of **central series**

$$1 \trianglelefteq \cdots \trianglelefteq A_{n-1} \trianglelefteq A_n \trianglelefteq A_{n+1} \trianglelefteq \cdots \trianglelefteq G$$

where we requires the successive quotient to be **central**, i.e., $[G, A_{n+1}] \leq A_n$, or equivalently, $A_{n+1} \diagup A_n \leq Z(G \diagup A_n)$, or equivalently, $xyA_n = yxA_n \in G \diagup A_n$ if one of x, y is in A_{n+1}.

To construct one, one can consider the **upper central series**, defining $G_{(n)} \triangleq [G, G_{(n-1)}]$ with $G_{(0)} \triangleq G$. This gives us

$$\cdots \trianglelefteq G_{(2)} \trianglelefteq G_{(1)} \trianglelefteq G$$

Note that

Theorem 1.6.1. (Every subgroup of a nilpotent group is subnormal) Let G be a nilpotent group with $H \leq G$. Then H is a subnormal subgroup of G.

Proof. Let

$$1 \triangleleft A_1 \triangleleft \cdots \triangleleft A_n = G$$

■

Corollary 1.6.2. (Nilpotent group satisfies normalizer condition) Let G be a nilpotent group. If $H < G$, then $H < N_G(H)$.

A group is said to be nilpotent if it admits a central series.

Equivalent Definition 1.6.3. (Nilpotency for finite group) Let G be a finite group. The followings are equivalent:

(i) G is nilpotent.

(ii) Sylow subgroups of G are all normal.

(iii) Sylow subgroups of G are all normal and they form an inner direct product equal to G.

(iv)

Proof. ■

1.7 Remarkable Exercises

Question 1: Wording problem

Let $n \in \mathbb{Z}$ satisfies

$$a^n = b^n \quad \text{and} \quad a^{n-1} = b^{n-1} \quad \text{and} \quad a^{n+1} = b^{n+1}, \quad \text{for all } a, b \in G$$

Show that G is abelian. fkjladslkfjadsfadsfjadsklfjadslkfjdas;lkfj;lk jdflk;jasdl;kfjsldkajf;lksdajflkjasdkl;fjadsk;lfjadl;skjfakl;fj;aldkfjals;dkf

Proof. Deduce

$$a^n b^n ab = (ab)^n (ab) = (ab)^{n+1} = a^{n+1} b^{n+1}$$

which implies

$$b^n a = ab^n$$

which implies

$$(a^{n-1} b^{n-1}) ba = a^n b^n = (a^{n-1} b^{n-1}) ab$$

as desired. ■

1.8 Exercises

For question 1, recall that by class equation, p-group can not have trivial center, and recall that G/N is abelian if and only if $[G,G] \leq N$.

Question 2

Show that

(i) If $H/Z(H)$ is cyclic, then H is abelian.

(ii) If H is of order p^2, then H is abelian.

From now on, suppose G is non-abelian with order p^3.

(iii) $|Z(G)| = p$.

(iv) $Z(G) = [G,G]$.

Proof. Let $a, b \in H$ and $H/Z(H) = \langle hZ \rangle$. Write $a = h^n z_1$ and $b = h^m z_2$. Because $z_1, z_2 \in Z(H)$, we may compute:

$$ab = h^n z_1 h^m z_2 = h^{n+m} z_1 z_2 = ba$$

as desired.

Let $|H| = p^2$. Because H is a p-group, we know $Z(H)$ is nontrivial, therefore either $|Z(H)| = p$ or $|Z(H)| = p^2$. To see the former is impossible, just observe that if so, then $|H/Z(H)| = p$, which implies $H/Z(H)$ is cyclic, which by part (i) implies $Z(H) = H$.

Because G is non-abelian, we know $|Z(G)| \neq p^3$. Because G is a p-group, we know $|Z(G)| \neq 1$. Therefore, either $|Z(G)| = p$ or $|Z(G)| = p^2$. Part (i) tell us that $|Z(G)| \neq p^2$, otherwise G is abelian, a contradiction. We have shown $|Z(G)| = p$, as desired.

We now prove $Z(G) = [G,G]$. Because $|Z(G)| = p$, by part (ii) we know $G/Z(G)$ is abelian. This implies $[G,G] \leq Z(G)$, which implies $[G,G]$ is either trivial or equal to $Z(G)$. Because G is non-abelian, we know $[G,G]$ can not be trivial. This implies $Z(G) = [G,G]$, as desired. ■

Question 3

(i) Let M, N be two normal subgroups of G with $MN = G$. Prove that

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

(ii) Let H, K be two distinct subgroups of G of index 2. Prove that $H \cap K$ is a normal subgroup with index 4 and $G/(H \cap K)$ is not cyclic.

Proof. The map $G/(M \cap N) \to (G/M) \times (G/N)$ defined by

$$g(M \cap N) \mapsto (gM, gN) \tag{1.1}$$

is clearly a well-defined group homomorphism, since if $gM = hM$ and $gN = hN$, then $gh^{-1} \in M$ and $gh^{-1} \in N$, which implies $gh^{-1} \in M \cap N$, which implies $g(M \cap N) = h(M \cap N)$. Let $gM = M$ and $gN = N$. Then $g \in M \cap N$ and $g(M \cap N) = M \cap N$. Therefore map 1.1 is also injective. It remains to show map 1.1 is surjective. Fix $g, h \in G$. Write $g = mn$ and $h = \widetilde{m}\widetilde{n}$. Clearly $gM = nM = \widetilde{m}nM$ and $hN = \widetilde{m}N = \widetilde{m}nN$. This implies that mapping 1.1 maps $\widetilde{m}n$ to (gM, hN), as desired.

Because H, K are both of index 2 in G, we know they are both normal in G. This by second isomorphism theorem implies HK forms a subgroup of G. Because $H \neq K$, we know HK properly contains H, which by finiteness of G implies the index of HK is strictly less than H, i.e., $HK = G$. Note that $H \cap K$ is normal since it is the intersection of normal subgroups. By part (i), we now have $G/(H \cap K) \cong (G/H) \times (G/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, which shows that $H \cap K$ has index 4 and $G/(H \cap K)$ is cyclic. ■

Question 4

Let G be a group of order pq, where $p > q$ are prime.

(i) Show that there exists a unique subgroup of order p.

(ii) Suppose $a \in G$ with $o(a) = p$. Show that $\langle a \rangle \subseteq G$ is normal and for all $x \in G$, we have $x^{-1}ax = a^i$ for some $0 < i < p$.

Proof. The third Sylow theorem stated that the number n_p of Sylow p-subgroups satisfies

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid q$$

Because $p > q$, together they implies $n_p = 1$. Since Sylow p-subgroups of G are exactly subgroups of order p, we have proved (i).

The third Sylow theorem also stated that $n_p = |G : N_G(P)|$ for any Sylow p-subgroup $P \leq G$. Therefore, $N_G(\langle a \rangle) = G$, i.e., $\langle a \rangle$ is normal in G. Fix $x \in G$. It remains to prove $xax^{-1} \neq e$, which is a consequence of the fact that conjugacy (automorphism) preserves order. ■

Question 5

Let H, K be two subgroups of G of coprime finite indices m, n. Show that

$$\operatorname{lcm}(m,n) \leq |G : H \cap K| \leq mn$$

Proof. Let $\Omega_{H\cap K}, \Omega_H$, and Ω_K respectively denote the set of left cosets of $H \cap K, H$, and K. The map $\Omega_{H\cap K} \to \Omega_H \times \Omega_K$ defined by

$$g(H \cap K) \mapsto (gH, gK) \tag{1.2}$$

is well defined since

$$g(H \cap K) = l(H \cap K) \implies g^{-1}l \in H \cap K \implies gH = lH \text{ and } gK = lK$$

such set map is injective since if $gH = lH$ and $gK = lK$, then $g^{-1}l \in H$ and $g^{-1}l \in K$, which implies $g(H \cap K) = l(H \cap K)$, as desired. From the injectivity of map 1.2, we have shown index of $H \cap K$ indeed have upper bound mn.

Because

$$|G : H \cap K| = |G : H| \cdot |H : H \cap K| = |G : K| \cdot |K : H \cap K|$$

we know both n and m divides $|G : H \cap K|$, which gives the desired lower bound $\operatorname{lcm}(m, n)$. ■

Question 6

(i) Let G be a group, $H \leq G$, and $x \in G$ of finite order. Prove that if k is the smallest natural number that makes $x^k \in H$, then $k \mid o(x)$.

(ii) Let G be a group and N a normal subgroup of G. Prove that

$$o(gN) = \inf \left\{ k \in \mathbb{N} : g^k \in N \right\}, \quad \text{where } \inf \varnothing = \infty$$

(iii) Let G be a finite group, H, N two subgroups of G with N normal. Show that if $o(H)$ and $|G : N|$ are coprime, then $H \leq N$.

Proof. (i): Let $a = qk + r \in \mathbb{N}$ with $0 \leq r < k$. If $x^a \in H$, then $x^r = x^a \cdot (x^k)^{-q} \in H$, which implies $r = 0$. We have shown that k divides all natural numbers a that makes $x^a \in H$, which includes $o(x)$.

(ii): This is a simple observation that $(gN)^k = g^k N \in N \iff g^k \in N$.

(iii): By second isomorphism theorem, we know $|HN : N| = |H : H \cap N|$ which divides both $o(H)$ and $|G : N|$. This by coprimality implies $|H : H \cap N| = 1$, which shows that $H \leq N$. ■

Question 7

Let G be a finite group with Sylow p-subgroup P and normal subgroup N. Show that $P \cap N$ forms a Sylow p-subgroup of N, and use such to deduce N have index $p^{\nu_p(o(PN))-\nu_p(o(N))}$ in PN.

Proof. By second isomorphism theorem, we have

$$o(PN) \cdot o(P \cap N) = o(P) \cdot o(N)$$

Because P is Sylow with $P \subseteq PN$, we know

$$\nu_p(o(PN)) = \nu_p(o(P))$$

This shows that, indeed, $P \cap N$ forms a Sylow p-subgroup of N:

$$\nu_p(o(P \cap N)) = \nu_p(o(N))$$

as desired. Because $P \cap N \leq P$ and because P is Sylow, we know $o(P \cap N)$ is a power of p. It then follows that:

$$|PN : N| = \frac{o(PN)}{o(N)} = \frac{o(P)}{o(P \cap N)} = p^{\nu_p(o(P))-\nu_p(o(P\cap N))} = p^{\nu_p(o(PN))-\nu_p(o(P))}$$

■

Question 8

Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

Proof. The facts that:

(i) By second isomorphism theorem, we have $|N : H \cap N| = |HN : H|$, which divides $|G : H|$.

(ii) $o(H \cap N) \mid o(H)$.

(iii) $o(H)$ and $|G : H|$ are coprime.

implies $o(H \cap N)$ and $|N : H \cap N|$ is coprime, i.e., $H \cap N$ is Hall in N.

The facts that:

(i) $o(HN/N) = \frac{o(HN)}{o(N)} = \frac{o(H)}{o(H \cap N)}$ divides $o(H)$. (second isomorphism theorem)

(ii) $|(G/N) : (HN/N)| = |G : HN|$ divides $|G : H|$.

(iii) $o(H)$ and $|G : H|$ are coprime.

implies $o(HN/N)$ and $|(G/N) : (HN/N)|$ are coprime, i.e., HN/N is Hall in G/N.

■

1.9 Exercises II

Question 9: subgroup of p-group of index p is normal

Prove that if p is a prime and $o(G) = p^\alpha$ with $\alpha \in \mathbb{N}$, then every subgroup H of index p is normal.

Deduce that every group of order p^2 has a normal subgroup of order p.

Proof. Let G acts on the left cosets spaces Ω of H. We have a group homomorphism $\varphi : G \to \text{Sym}(\Omega)$. Clearly we have $\ker \varphi \subseteq H$. By first isomorphism theorem, we know

$$|G : \ker \varphi| = o(\text{Im}\,\varphi) \mid \text{Sym}(\Omega)$$

Noting that $|\text{Sym}\,\Omega| = p!$, we see $\ker \varphi$ has index $\leq p$, which when combined with the fact $\ker \varphi \subseteq H$ shows that $H = \ker \varphi$, as desired.

Suppose $\alpha = 2$. By first Sylow theorem, there is a subgroup of G of order p. This subgroup is normal from what we have just proved. ■

Question 10

Let G be a group of odd order. Prove that for any $x \neq e \in G$, we have $\text{Cl}(x) \neq \text{Cl}(x^{-1})$.

Proof. Assume for a contradiction that $\text{Cl}(x) = \text{Cl}(x^{-1})$. Because $(gxg^{-1})^{-1} = gx^{-1}g^{-1} \in \text{Cl}(x^{-1}) = \text{Cl}(x)$, the inversion is well defined on $\text{Cl}(x)$, and moreover clearly bijective. Because $o(G)$ is odd, we may pair up the elements of $\text{Cl}(x)$ via inversion to see $|\text{Cl}(x)|$ is even. This is impossible since by orbit-stabilizer theorem, $|\text{Cl}(x)|$ is the index of some subgroup of G . ■

Question 11

Let $o(G) = p^n$ with $n \geq 3$ and $o(Z(G)) = p$. Prove that G has a conjugacy class of size p.

Proof. Class equation stated that

$$o(G) = o(Z(G)) + \sum |\text{Cl}(x)| \tag{1.3}$$

and the orbit stabilizer theorem shows that $|\text{Cl}(x)|$ is of order powers of p. If they are of p-powers ≥ 2, then we see

$$0 \equiv o(G) \equiv p \equiv o(Z(G)) + \sum |\text{Cl}(x)| \pmod{p}$$

a contradiction. ■

Question 12

Prove that if the center of G is of index n, then every conjugacy class has at most n elements.

Proof. Let $x \in G$. Because $Z(G) \subseteq C_G(x)$, by orbit-stabilizer theorem, we have:

$$|\mathrm{Cl}(a)| = |G : C_G(a)| \leq |G : Z(G)| = n$$

■

Question 13

Let $H, K \subseteq G$ be two finite subgroups. Show that

$$|HK| = \frac{o(H)o(K)}{o(H \cap K)}$$

Remark: The hint give a rigorous proof, but I prefer a heuristic one.

Proof. Consider the right coset spaces $\Omega \triangleq \{Hx : x \in G\}$, and let K acts on Ω by right multiplication. Because $Hk = H$ if and only if $k \in H$, we know the stabilizer subgroup K_H is identical to $K \cap H$. Therefore, by orbit-stabilizer theorem, we have

$$\frac{o(K)}{o(H \cap K)} = |\{Hk : k \in K\}|$$

Define an equivalence class in K by setting $k \sim \widetilde{k} \overset{\triangle}{\iff} Hk = H\widetilde{k}$. Pick a representative element our of each class and collect them into a set T. Clearly

$$|T| = |\{Hk : k \in K\}|$$

and we have a natural bijection $H \times T \to HK$. This finishes the proof. ■

Question 14

Let G be a non-abelian group of order 21. Prove that $Z(G) = 1$.

Proof. If $o(Z(G)) = 3$ or 7, then because $G/Z(G)$ is cylic ■

Question 15

Find all finite groups which have exactly two conjugacy classes.

Proof. Let G be a finite group that has exactly two conjugacy classes. One of the conjugacy class is $\{e\}$. Let a be an element of the other class. By class equation and orbit-stabilizer theorem, we have

$$|G| - 1 = |\mathrm{Cl}(a)| \mid o(G)$$

This implies $|G| = 2$, which implies $G = \mathbb{Z}_2$. ■

Question 16

Let H be a subgroup of G and let

$$\bigcup_{g \in G} gHg^{=1} = G$$

Show that $H = G$.

1.10 Exercises III

Question 17

Let $o(G) = 60$. Show that if G is simple, then G must have exactly 24 elements of order 5 and 20 elements of order 3.

Proof. By sylow, we have

$$n_5 \equiv 1 \pmod 5 \quad \text{and} \quad n_5 \mid 12$$

which by simplicity of G implies $n_5 = 6$. The same argument gives us $n_3 \in \{4, 10\}$. To see $n_3 \neq 4$, just recall that second sylow stated that conjugacy action $G \longrightarrow \text{Sym}(\text{Syl}_3(G)) \cong S_{n_3}$ is nontrivial, and is therefore injective by simplicity of G. We now see that $n_3 = 4$ is too small to satisfies

$$o(G) = 60 \mid n_3!$$

■

Question 18

Let $o(G) = pqr$ with $p < q < r$ prime. Prove that G has a normal Sylow r-subgroup H.

Proof. By sylow and counting arguments we know $1 \in \{n_p, n_q, n_r\}$. Therefore, if neither of n_p and n_q is 1, we are done. Suppose $1 \in \{n_p, n_q\}$. Either way, we get a normal subgroup N such that $o(G/N) \in \{qr, pr\}$. We also get a normal $H/N \in \text{Syl}_r(G/N)$. This give us a characteristic $K \in \text{Syl}_r(H)$, which is normal in G. ■

Question 19

Let $o(G) = p^3q$ with p, q prime. Show that one of the followings statement is true:

(i) G has a normal Sylow p-subgroup.

(ii) G has a normal Sylow q-subgroup.

(iii) $p = 2$, $q = 3$.

Proof. Suppose (i) and (ii) are both false. Then by sylow we have $n_p = q$ and $p < q$. Because $p < q$, applying sylow again we have $n_q \in \{p^2, p^3\}$. Because $n_p > 1$, by counting we see that $n_q \neq p^3$. Therefore $n_q = p^2$. Then by sylow, $p^2 = n_q \equiv 1 \pmod q$, which implies $q \mid (p-1)(p+1)$. Because $p < q$ and q is prime, we now see $q = p + 1$, which can only happens if $p = 2$ and $q = 3$. ■

Question 20

Show that no group of order 30 is simple.

Proof. Consider n_3 and n_5. We have $n_5 \in \{1,6\}$ and $n_3 \in \{1,10\}$. If $n_5 \neq 1 \neq n_3$, then there are 24 elements of order 5 and 20 elements of order 3, impossible for a group of order 30. ■

Question 21

Let G be a finite group with sylow p-subgroup P and normal subgroup N. Show that $P \cap N$ is p-sylow in N and that PN/N is p-sylow in G/N.

Proof. Second isomorphism theorem implies that

$$o(PN) \cdot o(P \cap N) = o(P) \cdot o(N)$$

Because P is p-sylow, we know $o(P)$ and $o(PN)$ has the same p-power, which implies that $o(P \cap N)$ and $o(N)$ has the same p-power, as desired. Again counting the p-power of $PN/N \subseteq G/N$, we see PN/N is p-sylow. ■

Question 22

Let G be a finite group, $H \leq G$ a subgroup with $[G : H] = n$. Show that:

(i) For all subgroup $K \leq G$, we have $[H : H \cap K] \leq [G : K]$.

(ii) $[H : H \cap H^g] \leq n$ for all $g \in G$.

(iii) If H is a maximal proper subgroup of G and H is abelian, show that $H \cap H^g \trianglelefteq G$ for all $g \notin H$.

(iv) Suppose that G is simple. If H is abelian and n is prime, then $H = 1$.

Proof. Let $H/H \cap K$ and G/K denote left coset spaces. (i) is a consequence of verifying that the function

$$H/H \cap K \longrightarrow G/K; \quad h(H \cap K) \mapsto hK$$

is well-defined and injective. (ii) is then a corollary of (i).

We now prove (iii). Fix $g \notin H$. There are two cases: Either $H = H^g$ or $H \neq H^g$. For the first case, just observe that by maximality of H, we will have $N_G(H) = G$. We now claim that $H \neq H^g \implies H \cap H^g \subseteq Z(G)$. Because H is abelian, we know $H \cap H^g \leq Z(H)$. Clearly we also have $H \cap H^g \leq Z(H^g)$. We now have $H \cap H^g \leq Z(\langle H, H^g \rangle)$, where

$\langle H, H^g \rangle = G$ by maximality of H, as desired.

We now prove (iv). Clearly the primality of n forces H to be a maximal proper subgroup of G. Therefore by (iii), $H \cap H^g = 1$ for all $g \notin H$. This by (ii) implies $n \le o(G) \le n^2$. Write $o(G) \triangleq nk$ so $k \in \{1, \dots, n\}$. We wish to show $k = 1$. To see $k \ne n$, just recall that if so, then G would be abelian, contradicting to its simplicity. To see $k \notin \{2, \dots, n-1\}$, just observe that if so, then the unique n-Sylow subgroup would be proper, contradicting to simplicity of G. ■

Question 23

Let G be a finite group with $P \in \mathrm{Syl}_p(G)$. Suppose that N is a normal subgroup of G with $[G : N] = o(P) > 1$. Show that

(i) N is the subset of G consisting of all elements of order not divisible by p.

(ii) If the elements of $G - N$ all has p-power order, then $P = N_G(P)$.

Proof. Because P is p-sylow and $[G : N] = o(P)$, we know $p \nmid o(N)$. This implies that no element of N has order divisible by p. Let $g \in G$ with $p \nmid o(g)$. To see that $g \in N$, just observe that because $o(gN) \mid o(g)$ and $o(gN)$ is a power of p, we have $o(gN) = 1$.

Assume for a contradiction that $P < N_G(P)$. Then there exists some nontrivial sylow q-subgroup Q of $N_G(P)$ with $q \ne p$. By definition we have $[Q, P] \le P$. By (i), $Q \le N$. Therefore we also have $[Q, P] \le N$. Coprimality of orders of N and P now tell us that $[Q, P] = 1$. We now see that the product of two nontrivial elements $x \in Q, y \in P$ has order divisible by pq, a contradiction to the premise. ■

1.11 Exercises IV

Question 24

Show that the center of products is a product of centers:

$$Z(G_1) \times \cdots \times Z(G_n) = Z(G_1 \times \cdots \times G_n)$$

Deduce that a direct product of groups is abelian if and only if each of its factor is abelian.

Proof. The "$\subseteq$" is clear. To see that

$$g_1 \times \cdots \times g_n \in Z(G_1 \times \cdots \times G_n) \implies g_i \in Z(G_i)$$

just observe that if not, then

$$[g_1 \times \cdots \times g_n, e_1 \times \cdots \times x_i \times \cdots \times e_n] \neq e \in \prod G_j$$

The second part then follows from noting

$$Z(G_1 \times \cdots \times G_n) = G_1 \times \cdots \times G_n \iff Z(G_i) = G_i, \quad \text{for all } i$$

■

Question 25

Let $G \triangleq A_1 \times \cdots \times A_n$ and $B_i \trianglelefteq A_i$ for all i. Prove that $B_1 \times \cdots \times B_n \trianglelefteq G$ and that

$$\frac{A_1 \times \cdots \times A_n}{B_1 \times \cdots \times B_n} = \frac{A_1}{B_1} \times \cdots \times \frac{A_n}{B_n}$$

Proof.

$$(g_1, \dots, g_n)(b_1, \dots, b_n)(g_1, \dots, g_n)^{-1} = (g_1 b_1 g_1^{-1}, \dots, g_n b_n g_n^{-1}) \in \prod B_i$$

The second part require us to show that

$$\prod \left(\frac{A_i}{B_i}\right) \longrightarrow \frac{\prod A_i}{\prod B_i}; \quad \prod \left(\frac{a_i}{B_i}\right) \mapsto \frac{\prod a_i}{\prod B_i}$$

is a well-defined group isomorphism, which boils down to showing that it is (i) well-defined, (ii) actually a homomorphism, (iii) injective, and (iv) surjective. To see it is injective, just observe that if $\prod a_i \in \prod B_i$, then $a_i \in B_i$ for all i, and therefore $\prod \frac{a_i}{B_i} = e$. The rest are clear. ■

Question 26

Let G be a finite abelian group with $m \mid o(G)$. Show that G has a subgroup of order m.

Proof. This follows from noting that if $o(a) = p^n$, then $o(a^{p^{n-d}}) = p^d$. (Ans also structure theorem for finite abelian group) ■

Question 27

Show that the subgroups and quotients of a nilpotent group G are also nilpotent.

Proof. Let H be a subgroup of G, and write

$$0 = G_{(n)} \trianglelefteq \cdots \trianglelefteq G_{(1)} \trianglelefteq G_{(0)} = G, \quad \text{with } G_{(k)} \triangleq [G, G_{(k-1)}]$$

To see that

$$0 \leq H_n \leq \cdots \leq H_1 \leq H$$

form a central series, where $H_k \triangleq H \cap G_{(k)}$, just observe that

$$[H, H \cap G_{(k)}] \leq H \text{ and } [H, H \cap G_{(k)}] \leq [G, G_{(k)}] \leq G_{(k-1)}$$

together implies

$$[H, H_k] \leq H \cap G_{(k-1)} = H_{k-1}$$

Let N be a normal subgroup of G, and let $m \leq n$ be the largest number such that $N \leq G_{(m)}$. It is clear that

$$\frac{N}{N} \leq \frac{G_{(m)}}{N} \leq \cdots \leq \frac{G_{(1)}}{N} \leq \frac{G}{N}$$

form a central series. ■

Question 28

Show that if $G/Z(G)$ is nilpotent, then G is nilpotent.

Proof. Consider the central series

$$\frac{Z(G)}{Z(G)} \trianglelefteq \frac{G_1}{Z(G)} \trianglelefteq \cdots \trianglelefteq \frac{G_n}{Z(G)} = \frac{G}{Z(G)}$$

Clearly we have the central series

$$0 \trianglelefteq Z(G) \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

■

Question 29

Let $o(G) = pqr$ with $p < q < r$ prime. Show that G is solvable.

Proof. Recall that we have a normal subgroup $M \in \mathrm{Syl}_r(G)$. Then we have a normal subgroup $\frac{H}{M} \in \mathrm{Syl}_q(G)$. Then $1 \trianglelefteq M \trianglelefteq H \trianglelefteq G$ forms the desired series. ■

Question 30

Show that a finite group G is nilpotent if and only if every $a, b \in G$ that makes $\gcd(o(a), o(b)) = 1$ also makes $ab = ba$.

Proof. ($\implies$): Write $G = P_1 \times \cdots \times P_n$ with P_i sylow. Clearly if the orders of $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are coprime to each other, then for all i, we must have either $x_i = e$ or $y_i = e$. This implies the commutativity.

($\impliedby$): We need to show that Sylow subgroups of G are normal. Let $P_1, \dots, P_n$ each be a Sylow subgroup of G with distinct p. By premise, we see that $P_k \subseteq N_G(P_1)$ for all $k \geq 2$. This then implies $G = N_G(P_1)$, as desired. ■

Question 31

Let $G = HK$ be finite and $S \leq G$ be a p-subgroup that contains some p-Sylow subgroup P of H and some p-Sylow subgroup Q of K. Show that

(i) S is p-Sylow in G.

(ii) $S = (S \cap H)(S \cap K)$

Proof. Because $P \cap Q \leq H \cap K$, we know p-part of

$$o(G) = \frac{o(H)o(K)}{o(H \cap K)}$$

is smaller than

$$\frac{o(P)o(Q)}{o(P \cap Q)} = |PQ| \leq o(S)$$

which can only happen if S is Sylow with $|PQ| = o(S)$. By definition, $P \leq S \cap H \leq H$. Because S is a p-group, we know $S \cap H$ is also a p-group. Sylowness of $P \leq H$ then forces $S \cap H = P$. Similarly, we have $S \cap K = Q$. Now, to see $S = PQ$, just recall that $|PQ| = o(S)$ ■

Question 32

Let $M \trianglelefteq G$ and $N \trianglelefteq G$ with M, N finite and nilpotent. Prove that MN is nilpotent.

Proof. The proof follows form noting that if $S \in \mathrm{Syl}_p(MN)$, then by earlier questions, S is uniquely determined by $S = (M \cap S)(N \cap S)$ with $M \cap S \in \mathrm{Syl}_p(M)$ and $N \cap S \in \mathrm{Syl}_p(N)$ uniquely determined. ■

Question 33

Let G be finite with $A, B \trianglelefteq G$ and $G/A, G/B$ solvable. Prove that $G/(A \cap B)$ is solvable.

Proof. ■