Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 12, 2020

Supplementary Problems.

1. a) If G is a finite abelian group with elements $a_1, a_2, \cdots, a_n$, prove that $a_1 a_2 \cdots a_n$ is an elements whose square is the identity.

Proof. We can make pairs (a, b) for each $a \in G$ where a and b are in inverse relationship with each other. In re-ordering $a_1 a_2 \cdots a_n$, this results out as the product of elements of order 2. In squaring, we have the identity. $\square$

b) If the G in part a) has no element of order 2 or more than one element of order 2, prove that $a_1 a_2 \cdots a_n = e$.

Proof. If G has no elements of order 2, then by the assertion made in a), we get $a_1 a_2 \cdots a_n = e$ clearly. If G has more than one element of order 2, without lossing of generality, we can assume that G is the group of elements of order 2 only. So, $o(G) = 2^n$ for some n. Let H be a subgroup of G with order 2^{n-1}(Such H always exists). Then $[G : H] = 2$ so that $G = xH \coprod H$. So for each $h \in H$, there corresponds a xh so that $xh \cdot h = xh^2 = x$. Hence, the product of all elements in G is $x^{2^{n-1}}$, where 2^{n-1} is even. Therefore, it is exactly the identity element. $\square$

c) If G has one element, y, of order 2, prove that $a_1 a_2 \cdots a_n = y$.

Proof. Following the assertion made in a), the product $a_1 a_2 \cdots a_n$ results out as the product of elements of order 2. In our case, it is y alone. $\square$

d) (Wilson's theorem) If p is a prime number show that $(p-1)! \equiv -1(p)$.

Proof. Consider $G = U_p$. Note that $p - 1$ is the only element in U_p with order 2(In fact, since U_p is cyclic, there must be exactly one element of order d where $d \mid p - 1$). Hence, applying the Problem c), we have $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$. $\square$

2. If p is an odd prime and if

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

where a and b are integers, prove that $p \mid a$. If $p > 3$, prove that $p^2 \mid a$.

Proof. Let

$$s = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

Since for each $\frac{1}{i} + \frac{1}{p-i} = \frac{p}{i(p-i)}$, we can rewrite s as

$$s = \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i(p-i)}.$$

Consequently, on mod p,

$$s \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i(p-i)} \equiv -\sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i^2} \equiv p \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \equiv p \sum_{i=1}^{\frac{p-1}{2}} i^2$$

so that $p^2 \mid s$ if $p > 3$. As $p \nmid b$, $p^2 \mid a$. Hence proved. □

3. If p is an odd prime, $a \neq 0$ (p) is said to be a quadratic residue of p if there exists an integer x such that $x^2 \equiv a \pmod{p}$. Prove
a) The quadratic residues of p form a subgroup Q of the group of nonzero integers mod p under multiplication.

Proof. As Q must be a finite set, it is enough to see that elements in Q are closed under mod p multiplication. Let $a, b \in Q$. Then there exists integers x, y such that

$$x^2 \equiv a \pmod{p}, \quad y^2 \equiv b \pmod{p} \implies (xy)^2 \equiv ab \pmod{p}.$$

Hence, $ab \in Q$ and Q is a subgroup(of U_p). □

b) $o(Q) = (p-1)/2$.

Proof. Consider a homomorphism $\phi : U_p \to Q$ defined by $\phi(x) = x^2$. This is a well-defined onto isomorphism(as p is an odd order prime) with kernel $K = \{1, p-1\}$. Consequently, G/K is isomorphic to Q with order $(p-1)/2$. That is, $o(Q) = (p-1)/2$. □

c) If $q \in Q$, $n \notin Q$ (n is called a non-residue), then nq is a nonresidue.

Proof. Note that Q is a normal subgroup of U_p since $[U_p : Q] = 2$. Hence, a coset decomposition

$$U_p = Q \coprod nQ \quad \text{where } n \notin Q$$

is possible. Thus, nq is always a nonresidue. □

d) If n_1, n_2 are nonresidues, then $n_1 n_2$ is a residue.

Proof. Note that from c), every nonresidues are of the form nq, where n is a nonresidue and $q \in Q$. Hence, $n_1 = nq_1$, $n_2 = nq_2$ for some $q_1, q_2 \in Q$. Thus,

$$n_1 \cdot n_2 = nq_1 \cdot nq_2 = n^2(q_1 q_2) \in Q$$

so that $n_1 n_2$ is also a residue. □

e) If a is a quadratic residue of p, then $a^{\frac{p-1}{2}} \equiv 1(p)$.

Proof. Since $o(Q) = (p-1)/2$, $a^{o(Q)} = a^{\frac{p-1}{2}} = 1 \pmod{p}$. □

4. Prove that in the integers mod p, p a prime, there are at most n solutions of $x^n \equiv 1(p)$ for every integer n.

Proof. We prove a more general statement by induction. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n. We claim that $f(x) = 0$ has at most n solutions for every integer n. The case $n = 1$ is trivial. So we assume that the statement is true for $n = k-1$. Set $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$. If f has no solutions, we are done. If f has $x = r$ as a solution,

$$\begin{aligned} f(x) - f(r) &= a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0 - (a_n r^k + a_{k-1} r^{k-1} + \cdots + a_1 r + a_0) \\ &= a_k(x^k - r^k) + a_{k-1}(x^{k-1} - r^{k-1}) + \cdots a_1(x - r) \\ &= (x - r)g(x) \end{aligned}$$

for some polynomial $g(x)$ of degree $k-1$. This relation holds over any field. Assuming the mod p calculation, as $g(x) = 0$ has at most $k-1$ solutions, $f(x)$ has at most k solutions mod p. Thus, by induction, setting $f(x) = x^n - 1$ we have the required result. □

5. Prove that the nonzero integers mod p under multiplication form a cyclic group if p is a prime.

Proof. We know that U_p is a finite abelian group. Applying both Problem 4 above and Problem 38 of Section 2.4 2.5, U_p is a cyclic subgroup. □

6. Give an example of a non-abelian group in which $(xy)^3 = x^3 y^3$ for all x and y.

Proof. Consider the 3-Sylow subgroup of $GL(3, \mathbb{Z}_3)$

$$P_3 = \left\{ \begin{pmatrix} 1 & z_1 & z_2 \\ 0 & 1 & z_3 \\ 0 & 0 & 1 \end{pmatrix} \middle| z_i \in \mathbb{Z}_3, i = 1, 2, 3 \right\}.$$

It is a non-abelian group since

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Also, every element of P_3 has order 3 since

$$\begin{pmatrix} 1 & z_1 & z_2 \\ 0 & 1 & z_3 \\ 0 & 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3z_1 & 3z_2 + 3z_1 z_3 \\ 0 & 1 & 3z_3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for all $u_i \in \mathbb{Z}_3$. Thus, the equation $(xy)^3 = x^3 y^3$ is clearly satisfied. Hence, P_3 is the group we seek. □

7. If G is a finite abelian group, prove that the number of solutions of $x^n = e$ in G, where $n \mid o(G)$ is a multiple of n.

Proof. Refer the Problem 8. □

8. Same as Problem 7, but do not assume the group to be abelian.

Proof. This is also known as Frobenius Theorem. Check: Frobenius, G. (1903), "Über einen Fundamentalsatz der Gruppentheorie", Berl. Ber.: 987–991, JFM 34.0153.01. □

9. Find all automorphisms of S_3 and S_4, the symmetric groups of degree 3 and 4.

Solution. We rather prove a more general result, that $\mathscr{A}(S_n) \simeq S_n$ except for $n = 6$. This proof is a copy of a paper by IRVING E. SEGAL.
Let A be a automorphism of S_n. Then A takes a class of similar elements(conjugate class) into a class of similar elements. That is, it takes an element of order m to element of same order. Suppose $(1, r)A = t_1(r) \cdots t_k(r), k \geq 1$ where each t_i are disjoint transpositions. There are $\dfrac{n(n-1)}{2}$ conjugates of $(1, 2)$ and $\dfrac{n!}{2^k k!(n-2k)!}$ conjugates of $t_1(r) \cdots t_k(r)$. Hence,

$$\frac{n(n-1)}{2} = \frac{n!}{2^k k!(n-2k)!}.$$

If $n \neq 6$ this equation is satisfied for no k, except $k = 1$. Suppose that $n \neq 6$. Then $(1, r)A = (a_r, b_r)$. If $r \neq 2$, $(1, 2)(1, r) = (1, 2, r)$ so that $(1, 2, r)A = (a_2, b_2)(a_r, b_r)$. Since $(1, 2, r)$ has order 3, so has $(a_2, b_2)(a_r, b_r)$ and the transpostions $(a_2, b_2)(a_r, b_r)$ must have a letter in common. WLOG, assume that $a_2 = a_r$ or $b_2 = b_r$. However if $a_2 = a_r$ and $b_2 = b_s, r \neq 2, s \neq 2$, then $r \neq s$ and $(1, 2, r)A = (1, 2)A \cdot (1, r)A = (a_2, b_2) \cdot (a_r, b_r) = (b_r, a_2, b_2)$. Similarly, $(1, 2, s)A = (a_s, b_2, a_2)$. Hence $((1, 2, r)(1, 2, s))A = (b_r, a_2, b_2)(a_s, b_2, a_2) = (b_r, a_s, b_2)$ which is of order 3, while $(1, 2, r)(1, 2, s) = (1, s)(1, r)$ is of order 2. Hence, one must have $a_2 = a_r$ for all r or $b_2 = b_r$ for all r. We let $a_2 = a_r$ for all $r = 2, 3, \cdots, n$, then $(1, r)A = (a_2, b_r)$. Hence A is precisely the automorphism A defined by $xA = t^{-1}xt$ where

$$t = \begin{pmatrix} 1 & 2 \cdots & r & \cdots & n \\ a_2 & b_2 \cdots & b_r & \cdots & b_n \end{pmatrix}.$$

For $xA = t^{-1}xt$ when $x = (1, r)$, and the elements $\{(1, r)\}$ generates S_n. □

10. Prove that a subgroup of a solvable group and the homomorphic image of a solvable group must be solvable.

Proof. Suppose G is solvable and

$$G = N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_{r-1} \rhd N_r = (e)$$

where N_i is normal in N_{i-1} and N_{i-1}/N_i is abelian. Let H be a subgroup of G. We know that $H \cap N_i$ is normal in $H \cap N_{i-1}$. Now by Second Isomorphism Theorem,

$$\frac{H \cap N_{i-1}}{H \cap N_i} \simeq \frac{(H \cap N_{i-1})N_i}{N_i},$$

and since $(H \cap N_{i-1})N_i \subset N_{i-1}$, $\dfrac{(H \cap N_{i-1})N_i}{N_i}$ is abelian. Thus,

$$H = H \cap N_0 \rhd H \cap N_1 \rhd H \cap N_2 \rhd \cdots \rhd H \cap N_{r-1} \rhd N_r = (e)$$

so that H is solvable.
Now we show that the homomorphic image of G is solvable. Let $\overline{G}$ denote the homomorphic image of a group G. Note that by Lattice Theorem(Third Isomorphism Theorem), for a homomorphism ϕ,

$$\frac{G}{N} \simeq \frac{\overline{G}}{\overline{N}}$$

where N is a normal subgroup of G so that $\overline{G} \simeq G/\ker\phi$ and $\overline{N} \simeq N/\ker\phi$. Hence, applying the theorem successively in the chain

$$\overline{G} = \overline{N_0} \rhd \overline{N_1} \rhd \cdots \rhd \overline{N_r} = (e),$$

we conclude that each $\overline{N_i}$ is normal in $\overline{N_{i-1}}$ and $\overline{N_{i-1}}/\overline{N_i}$ is abelian. Thus, the homomorphic image of G is solvable. □

11. If G is a group and N is a normal subgroup of G such that both N and G/N are solvable, prove that G is solvable.

Proof. Let us consider the subnormal chain of G/N and N given respectively by

$$G/N \rhd G_1' \rhd \cdots \rhd G_k' = N, \quad N \rhd N_1 \rhd \cdots \rhd N_r = (e).$$

Consider the subgroup G_i of G satisfying $G_i/N \simeq G_i'$. Now by Lattice Theorem,

$$\frac{G_{i-1}'}{G_i'} \simeq \frac{\frac{G_{i-1}}{N}}{\frac{G_i}{N}} \simeq \frac{G_{i-1}}{G_i}$$

so that the subnormal chain

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_k = N$$

is an abelian tower. Consequently, using that N is also solvable,

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_k = N \rhd N_1 \rhd \cdots \rhd N_r = (e).$$

Therefore, G is a solvable group. □

12. If G is a group, A a subgroup of G and N a normal subgroup of G, prove that if both A and N are solvable then so is AN.

Proof. Note that by Second Isomorphism Theorem,

$$\frac{AN}{N} \simeq \frac{A}{N \cap A}.$$

Since A is solvable, so does its subgroup $N \cap A$. Since $A/(N \cap A)$ is a homomorphic image of A and AN/N being an isomorphic copy of it, it is also solvable. Now applying the result of Problem 11, as AN/N and N are solvable, AN is solvable. □

13. If G is a group, define the sequence of subgroups $G^{(i)}$ of G by
1) $G^{(1)}$ = commutator subgroup of G = subgroup of G generated by all $aba^{-1}b^{-1}$ where $a, b \in G$.
2) $G^{(i)}$ = commutator subgroup of $G^{(i-1)}$ if $i > 1$.
Prove a) Each $G^{(i)}$ is a normal subgroup of G.

Proof. We prove by induction. We already know that commutator subgroups are normal in G. Suppose we assume that $G^{(i-1)}$ is normal in G, then for any $a, b \in G^{(i-1)}$, $g \in G$,

$$\begin{aligned} g(aba^{-1}b^{-1})g^{-1} &= ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \in G^{(i)} \end{aligned}$$

which implies that $G^{(i)}$ is normal in G. □

b) G is solvable if and only if $G^{(k)} = (e)$ for some $k \geq 1$.

Proof. Suppose G is solvable. That is, there exists a subnormal chain

$$G = N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_{k-1} \rhd N_k = (e)$$

where each N_i are normal in N_{i-1} and N_{i-1}/N_i is abelian. Note that $G^{(i)}$ is the subgroup of $G^{(i-1)}$ where if $G^{(i-1)}/N$ is abelian, then $G^{(i)} \subset N$. That is, commutator subgroups are the smallest subgroup in G making the quotient group abelian. Consequently, we have $G^{(1)} \subset N_1$. Since $G^{(1)}/N_2\ G^{(1)}$ being a subgroup of N_1, it is abelian and hence $G^{(2)} \subset N_2$. Thus, we can conclude that $G^{(k)} \subset N_k = (e)$ so that $G^{(k)} = (e)$.
Conversely, assume that $G^{(k)} = (e)$. Then we can construct a subnormal abelian tower

$$G = G \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(k)} = (e)$$

so that G is solvable. □

14. Prove that a solvable group always has an abelian normal subgroup $M \neq (e)$.

Proof. Assume that G is solvable. Then $G^{(k)} = (e)$ for some $k \geq 1$. Let this be the first to be equivalent to trivial group in the subnormal chain of commutator subgroups. Hence, $G^{(k-1)} \neq (e)$ and $G^{(k-1)}/G^{(k)} \simeq G^{(k-1)}$. Since $G^{(k-1)}/G^{(k)}$ must be abelian and $G^{(k-1)}$ being a normal subgroup of G, $G^{(k-1)}$ is the desired abelian normal subgroup of G. □

15. a) Show that each $G_{(i)}$ is a normal subgroup of G and $G_{(i)} \supset G^{(i)}$.

Proof. We make use of similar proof with Problem 13 a). We already know that commutator subgroups are normal in G. Suppose we assume that $G_{(i-1)}$ is normal in G, then for any $a \in G, b \in G_{(i-1)}$, $g \in G$,

$$\begin{aligned} g(aba^{-1}b^{-1})g^{-1} &= ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \in G_{(i)} \end{aligned}$$

which implies that $G^{(i)}$ is normal in G(by the induction process). Similarly, on induction, we assume that $G_{(i-1)} \supset G^{(i-1)}$. Note that for any $a, b \in G^{(i)}$, $aba^{-1}b^{-1} \in G_{(i)}$ since $a \in G$ and $b \in G^{(i-1)} \subset G_{(i)}$. Thus, $G_{(i)} \supset G^{(i)}$ holds for all i. □

b) If G is nilpotent, prove it must be solvable.

Proof. If G is nilpotent, $G_{(k)} = (e)$ for some integer k and $G^{(k)} \subset G_{(k)} = (e)$ so that $G^{(k)} = (e)$. Therefore, G is solvable. □

c) Give an example of a group which is solvable but not nilpotent.

Solution. Consider the symmetric group S_3. Then it is solvable since

$$S_3 \triangleright A_3 \triangleright (e)$$

but not nilpotent as $S_{3_{(i)}} = A_3$ for all $i = 1, 2, \cdots$ □

16. Show that any subgroup and homomorphic image of a nilpotent group must be nilpotent.

Proof. Let G be a nilpotent group and H be its subgroup. We claim that $H_{(i)} \subset G_{(i)}$ for all i. $H_{(1)} \subset G_{(1)}$ is trivial. So we assume that $H_{(i-1)} \subset G_{(i-1)}$. Now for any $aba^{-1}b^{-1} \in H_{(i)}$, where $a \in H, b \in H_{(i-1)}$, it follows that $a \in G, b \in G_{(i-1)}$ so that $aba^{-1}b^{-1} \in G_{(i)}$. Therefore, by induction, $H_{(i)} \subset G_{(i)}$ holds for all i. Since $G_{(k)} = (e)$ for some integer k, $H_{(k)} = (e)$ so that H is also nilpotent.
Now consider a homomorphism ϕ and its image $\phi(G)$. It is immediate that $\phi(G)_{(k)}$ is the image of $G_{(k)}$. Therefore, if $G_{(k)} = (e)$, then $\phi(G)_{(k)} = (e)$ so that $\phi(G)$ is nilpotent. □

17. Show that every homomorphic image, different from (e), of a nilpotent group has a nontrivial center.

Proof. Note that a homomorphic image of a nilpotent group is nilpotent. We claim that every non-trivial nilpotent group has a nontrivial center. Suppose a group G is nilpotent. Then $G_{(k)} = (e)$, $G_{(k-1)} \neq (e)$ for some integer k. Recall the definition of $G_{(k)}$:

$$G_{(k)} = \{aba^{-1}b^{-1} |\, a \in G, b \in G_{(k-1)}\}.$$

Consequently, $G_{(k)} = (e)$ implies that $aba^{-1}b^{-1} = e$ for all $a \in G$ and $b \in G_{(k-1)}$. Equivalently, $ab = ba$ for all $a \in G$, $b \in G_{(k-1)}$. Since $G_{(k-1)}$ is nontrivial, $(e) \subsetneq G_{(k-1)} \subset Z(G)$. This shows that nilpotent group G has a nontrivial center. □

18. a) Show that any group of order p^n, p a prime, must be nilpotent.

Proof. We make an induction on the size of group G. Suppose $o(G) = 1$, then it is clearly nilpotent. So we assume that the statement is true for any p-group with order less than $o(G) = p^n$. Note that every p-group has nontrivial center. Hence, $G/Z(G)$ is a p-group with order less then p^n, so it is nilpotent. We know that for any surjective homomorphism ϕ, the image of $G_{(k)}$ is exactly $\overline{G}_{(k)}$ where $\phi(G) = \overline{G}$. Consider the homomorphism $\phi : G \to G/Z(G)$, $g \mapsto gZ(G)$. Consequently, $\overline{G}_{(k)} = (G/Z(G))_{(k)} = (e)$ for some integer k implying $G_{(k)}/\ker\phi \simeq (e) \implies G_{(k)} \subset \ker\phi = Z(G)$. Therefore, $G_{(k+1)} = \{aba^{-1}b^{-1} |\, a \in G, b \in G_{(k)} \subset Z(G)\} = (e)$ so that G is nilpotent. □

b) If G is nilpotent, and $H \neq G$ is a subgroup of G, prove that $N(H) \neq H$ where $N(H) = \{x \in G |\, xHx^{-1} = H\}$.

Proof. Given H is a proper subgroup of G, there exists $G_{(k)}$ such that $G_{(k)} \subset H$ but $G_{(k-1)} \not\subset H$. Choose $g \in G_{(k-1)} - H$. By the definition of $G_{(k)}$, for any $h \in H$ $ghg^{-1}h^{-1} \in G_{(k)} \subset H$. Consequently, $ghg^{-1} \in H$ for all $h \in H$, implying $g \in N(H)$. Therefore, $N(H) \neq H$ if G is nilpotent. □

19. If G is a finite group, prove that G is nilpotent if and only if G is the direct product of its Sylow subgroups.

Proof. Suppose G is nilpotent. Let P be a p-Sylow subgroup of G. Set $H = N(P)$. We know that $N(N(P)) = N(P) \iff N(H) = H$. So, this forces us that $H = G = N(P)$, and hence P is normal in G. Let $o(G) = n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and P_i be the (normal) p_i-Sylow subgroups of G respectively. Consequently, $G = P_1 P_2 \cdots P_k$, so that G is the direct product of its Sylow subgroups.
Conversely, we assume that G is the direct product of its Sylow Subgroups. That is, without of lossing of generality, we can assume it to an outer product(up to isomorphism, in fact)

$$G = P_1 \times P_2 \times \cdots \times P_k.$$

Thus,

$$Z(G) = Z(P_1) \times Z(P_2) \times \cdots \times Z(P_k) \neq (e),$$
$$G/Z(G) = P_1/Z(P_1) \times P_2/Z(P_2) \times \cdots P_k/Z(P_k).$$

Note that $G/Z(G)$ is a group of order less than $o(G)$. So that by induction, it is nilpotent. Now, we apply the assertion made in Problem 18 a). We construct a homomorphism $\phi : G \to G/Z(G)$ by $g \mapsto gZ(G)$, so that $\overline{G}_{(k)} = (G/Z(G))_{(k)} = (e)$ for some integer k. Now we have that $G_{(k)} \subset Z(G)$, implying $G_{(k+1)} = (e)$. Thus, G is nilpotent. □

20. Let G be a finite group and H a subgroup of G. For A, B subgroups of G, define A to be conjugate of B relative to H if $B = x^{-1}Ax$ for some $x \in H$.Prove
a) This defines an equivalence relation on the set of subgroups of G.

Proof. (Reflexivity) $A = eAe^{-1}$ so that $A \sim A$.
(Symmetry) If $A \sim \iff B = hAh^{-1}$ for some $h \in H$, $A = h^{-1}Bh$ so that $B \sim A$.
(Transitivity) Suppose $A \sim B$ and $B \sim C$. Then $B = hAh^{-1}$ and $C = gBg^{-1}$ for some $h, g \in H$. Consequently, $C = (gh)A(gh)^{-1}$ so that $A \sim C$.
Hence, the relation $\sim$ defines an equivalence relation on the set of subgroups of G. □

b) The number of subgroups of G conjugate to A relative to H equals the index of $N(A) \cap H$ in H.

Proof. It is enough to show that $N_H(A) = N(A) \cap H$. Note that $g \in N_H(A)$ iff and only if $g \in H$ and $gAg^{-1} = A$ so that $g \in N(A)$. Hence, $N_H(A) = N(A) \cap H$. Clearly $[H : N_H(A)]$ is the number of subgroup of G conjugate to A relative to H. With the result above, we have $[H : N(A) \cap H] = [H : N_H(A)]$. □

21. a) If G is a finite group and if P is a p-Sylow subgroup of G, prove that P is the only p-Sylow subgroup in $N(P)$.

Proof. Note that P is a p-sylow subgroup of $N(P)$. Hence every conjugate of P under $N(P)$ is also a p-Sylow subgroup of $N(P)$. Choose any $g \in N(P)$. Since $gPg^{-1} = P$, conjugate of P under $N(P)$ is sorely P itself. Hence, P is the only p-Sylow subgroup of $N(P)$. □

† **Remark:** We can prove a more general statement: If G is a finite group and P is a p-Sylow subgroup of G, then for any p-subgroup H of $N(P)$ must lie in P. Observe that our proof this lemma does not require the Second Sylow Theorem.

Proof. In $N(P)$, P being the normal subgroup of $N(P)$, HP is a subgroup $N(P)$. Clearly, HP is also a p-group and since

$$|HP| = \frac{|H| \cdot |P|}{|H \cap P|} \leq o(P),$$

$H \subset H \cap P$ so that $H \subset P$. This implies that every p-Sylow subgroup of $N(P)$ is exactly P, so that P is the only p-Sylow subgroup of $N(P)$. □

b) If P is a p-Sylow subgroup of G and if $a^{p^k} = e$ then, if $a \in N(P)$, a must be in P.

Proof. Consider the subgroup (a). Note that (a) is a p-group contained in $N(P)$. Therefore we have that

$$|(a)P| = \frac{|(a)| \cdot |P|}{|(a) \cap P|} \leq o(P)$$

so that $(a) \subset (a) \cap P \implies (a) \subset P$. Thus, $a \in P$. □

c) Prove that $N(N(P)) = N(P)$.

Proof. It is easy to see that $N(P) \subset N(N(P))$. Now, choose $g \in N(N(P))$. Observe that

$$gPg^{-1} \subset gN(P)g^{-1} = N(P)$$

so that $gPg^{-1} = P$. Hence, $g \in N(P)$ and $N(N(P)) = N(P)$. □

22. a) If G is a finite group and P is a p-Sylow subgroup of G, prove that the number of conjugates of P in G is not a multiple of p.

Proof. Let $C(P)$ denote the set of conjugates of P in G. We know that $o(G) = |C(P)| \cdot o(N(P))$. Since $P \subset N(P)$, $o(G)/o(N(P))$ does not have p as an divisor. Therefore, $p \nmid |C(P)|$. $\square$

b) Breaking up the conjugate class of P further by using conjugacy relative to P, prove that the conjugate class of P has $1 + kp$ distinct subgroups.

Proof. Let S be the set of all conjugates of P of G, where P is a p-Sylow subgroup. In one's heart, it is clear that $o(gPg^{-1}) = o(P)$ so that every conjugates of P is also a p-Sylow subgroup of G. Now consider a normal conjugation group action from P to S(This is what exactly the notion of relative conjugacy interpreted in the terms of group actions). If we denote the conjugacy class of $S_0 \in S$ under P as $C_P(S_0)$, we have

$$|S| = \sum_{S' \in S} \left| C_P(S') \right|.$$

In particular, we consider $C_P(P)$. It is trivial that $C_P(P) = \{P\}$ and hence, $|C_P(P)| = 1$. Can there be any other p-Sylow subgroup S' satisfies $|C_P(S')| = 1$? Suppose $|C_P(S')| = 1$. This implies that $P \subset N(S')$. Since $S' \subset N(S')$, both P and S' being a p-Sylow subgroup of G, it is must that $P = S'$. Thus, there is no p-Sylow subgroup other than P with conjugate class size 1. Now by Orbit-Stabilizer Theorem, size of $C_P(S')$ must be a power of p, so that $p \mid C_P(S')$ for all p-Sylow subgroup S'. Ultimately,

$$|S| = \sum_{S' \in S} \left| C_P(S') \right| = 1 + \sum_{S' \neq P \in S} \left| C_P(S') \right| = 1 + kp$$

for some integer k. As $|S|$ being the number of distinct conjugates of P of G, equivalently, we have shown that size of the conjugate class of P is $1 + kp$. $\square$

23. a) If P is a p-Sylow subgroup of G and B is a subgroup of G of order p^k, prove that if B is not contained in some conjugate of P, then the number of conjugates of P in G is a multiple of p.

Proof. We take the notation used in the Problem 22 b). Now we consider a normal conjugation group action from B to S. Recall that $C_B(S')$ has size 1 if and only if B is contained in S', that is, B lies in one of the conjugate of P. But this is a contradiction. Thus, every conjugacy class has size larger than 1, so that p divides its size. Since $|S|$ being the sum of sizes of whole conjugacy classes, $p \mid |S|$. $\square$

b) Using part a) and Problem 22, prove that B must be contained in some conjugate of P.

Proof. Problem 22 b) implies that the conjugate class of P has size of $1+kp$ while Problem 23 a) says that it must have p as a divisor. So, it forces us that B is contained in one of the conjugates of P. $\square$

c) Prove that any two p-Sylow subgroups of G are conjugate in G.

Proof. Take B as an arbitrary p-Sylow subgroup of G. Then the result is straightforward. □

24. Combine Problems 22 and 23 to give another proof of all parts of Sylow's Theorem.

Proof. Problem 23 c) is the exact statement of Second Sylow Theorem. Now from this, we know that every p-Sylow subgroups of G are conjugate so that by the result of Problem 22 b), there are $1 + kp$ distinct p-Sylow subgroups in G. This gives the another proof of Third Sylow Theorem. □

25. Making a case-by-case discussion using the result developed in this chapter, prove that any group of order less than 60 either is prime order of has a nontrivial normal subgroup.

Proof.

- $o(G) = 1$: Trivial
- $o(G) = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$: G is of prime order.
- $o(G) = 4, 8, 9, 16, 25, 27, 32, 49$: G is of order p^n, $n > 1$. So it has normal subgroups of order p^{n-1}.
- $o(G) = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 51, 55, 57, 58$: G is of order pq, where p, q are distinct prime and $p < q$. Then G has a normal q-Sylow subgroup.
- $o(G) = 12, 18, 20, 28, 44, 45, 50, 52$: G is of order p^2q, where p, q are distinct primes. Then G has either a normal p-Sylow subgroup or a normal q-Sylow subgroup.
- $o(G) = 30, 42$: G is of order p, q, r where p, q, r are distinct primes and $p < q < r$. Then G has a normal r-Sylow subgroup.
- $o(G) = 24$: Let P_2 be the 2-Sylow subgroup of G. Then $o(P_2) = 8$ and hence $24 \nmid [G : P_2] = 3! = 6$, so that P_2 must contain a nontrivial normal subgroup of G.
- $o(G) = 40$: Let P_5 be the 5-Sylow subgroup of G. since $1 + 5k \mid 8$ for $k = 1$ only, P_5 is normal in G.
- $o(G) = 48$: Let P_2 be the 2-Sylow subgroup of G. Then $o(P_2) = 16$ and hence $48 \nmid [G : P_2] = 3! = 6$, so that P_2 must contain a nontrivial normal subgroup of G.
- $o(G) = 54$: It has a normal 3-Sylow subgroup as its index in G is 2.
- $o(G) = 56$: If it has normal 7-Sylow subgroup, then it is done. If not, then it must have 8 disitnct 7-Sylow subgroups, so that G has 48 elements of order 7. There are 8 elements left for G and since the order of 2-Sylow subgroup is 8, 2-Sylow subgroup is the required normal subgroup of G.

□

26. Using the result of Problem 25, prove that any group of order less than 60 is solvable.

Proof. If a group G is abelian or of order p^n where p is a prime, then G is solvable. Also, we make use of the result of Problem 11 to check the solvability of G.

- $o(G) = 1$: Trivial
- $o(G) = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59$: G is of order p^n. Hence solvable.
- $o(G) = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 51, 55, 57, 58$: G is of order pq, so has a normal q-Sylow subgroup Q. Also, the order of G/Q is prime, hence G/Q is solvable. Applying Problem 11, G is solvable.
- $o(G) = 12, 18, 20, 28, 44, 45, 50, 52$: G is of order p^2q, where p, q are distinct primes. Then G has either a normal p-Sylow subgroup or a normal q-Sylow subgroup. Let N be the normal Sylow subgroup. Then G/N has order p^2 or q, which implies that G/N is solvable. Consequently, G is solvable.
- $o(G) = 30, 42$: G is of order p, q, r where p, q, r are distinct primes and $p < q < r$. Then G has a normal r-Sylow subgroup R. Then G/R is a group of order pq, so that it is solvable. Thus, G is solvable.
- $o(G) = 24$: G contains a nontrivial normal subgroup of order 2^k, $k \leq 3$. Then G/N is a group of order $3, 2 \cdot 3, 2^2 \cdot 3$ where in any cases, it is solvable. Hence, G is also solvable.
- $o(G) = 40$: The 5-Sylow subgroup P_5 is normal in G, G/P_5 has order 2^3 so that G/P_5 is solvable. Thus, G is solvable.
- $o(G) = 48$: Let P_2 be the 2-Sylow subgroup of G. Then G/P_2 has order $3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3$. But in either cases G/P_2 is still solvable. So does G.
- $o(G) = 54$: G has normal 3-Sylow subgroup with index 2. Thus, G is solvable.
- $o(G) = 56$: If it has normal 7-Sylow subgroup P_7, G/P_7 is a group of order 8 and hence solvable. If it has normal 2-Sylow subgroup P_2, G/P_2 is a group of order 7. So in either cases, G is solvable.

$\square$

27. Show that the equation $x^2ax = a^{-1}$ is solvable for x in the group G if and only if a is the cube of some element in G.

Proof. Multiplying ax^{-1} on the left and ax on the right of the given equation,

$$(ax^{-1})x^2ax(ax) = (ax^{-1})a^{-1}(ax) \iff (ax)^3 = a$$

so that a is a cube of some element in G. Conversely, assume that $a = b^3$ for some $b \in G$. Let $x = a^{-1}b$. Then

$$\begin{aligned} x^2ax &= (a^{-1}b)^2a(a^{-1}b) \\ &= a^{-1}ba^{-1}b^2 \\ &= a^{-1}ba^{-1}b^2(b \cdot b^{-1}) \\ &= a^{-1}ba^{-1}ab^{-1} = a^{-1}. \end{aligned}$$

Therefore, we conclude that the given equation is solvable if and only if a is a cube of an element in G. □

28. Prove that $(1,2,3)$ is not a cube of any element in S_n.

Proof. If $\sigma^3 = (1,2,3)$ for some $\sigma \in S_n$, then σ is a permutation of order 1,3 or 9.

- If $o(\sigma) = 1$, then $\sigma = e$, a contradiction.
- If $o(\sigma) = 3$, then σ is a product of disjoint 3 cycles. But on cubing the 3-cycles we get an identity. Therefore a contradiction.
- If $o(\sigma) = 9$, then σ is a product of disjoint 3 cycles with at least one or more 9 cycles. But on cubing this, the 3 cycles vanishes while the 9 cycle results out with product of 3 disjoint 3 cycles, which is again a contradiction.

Therefore, $(1,2,3)$ is not a cube of any element in S_n. □

29. Prove that $xax = b$ is solvable for x in G if and only if ab is the square of some elements in G.

Proof. Multiplying a on left of the equation we have $axax = ab \iff (ax)^2 = ab$. Conversely, if $ab = t^2$ for some $t \in G$, let $x = a^{-1}t$ so that

$$xax = (a^{-1}t)a(a^{-1}t) = a^{-1}(ab) = b.$$

Thus, $xax = b$ is solvable for x in G if and only if ab is the square of some elements in G. □

30. If G is a group and $a \in G$ is of finite order and has only a finite number of conjugates in G, prove that these conjugates of a generate a finite normal subgroup of G.

Proof. Let $S = \{s_1, s_2, \cdots, s_k\}$ denote the set of all conjugates of a. Note that $o(s_i) = o(a)$. Let $o(a) = n$. Suppose (S) is the set generated by S. (S) is clearly a normal subgroup. We claim that (S) has finite order. If we choose $1 \neq s \in (S)$, then $s = s_{a_1}^{m_1} s_{a_2}^{m_2} \cdots s_{a_r}^{m_r}$ where $1 \leq a_i \leq k$. In general, there exists an expression of s with shortest length r, with one appears as the first in the lexicographic ordering of r-tuples $(a_1, a_2, \cdots, a_r)$. Since the given S is a normal subset, there can be shifts of ordering of s_i's in the expression of each element s. This forces us that $a_1 < a_2 \cdots < a_r$. Hence, there can be at most $\prod_{i=1}^{k} o(s_i) = n^k$ elements is (S). □

31. Show that a group cannot be written as the set-theoretic union of two proper subgroups.

Proof. Suppose $G = A \cup B$ where A, B are proper subgroups of G. Then $A \not\subset B$ and $B \not\subset A$. So, choose $a \in A - B$ and $b \in B - A$. Clearly, $ab \in G$ so that $ab \in A$ or $ab \in B$. Suppose $ab \in A$. Then $a^{-1}ab = b \in A$. But by the definition of b, $b \notin A$, a contradiction. Hence $ab \notin A$. Similarly, $ab \notin B$ either. But this contradicts that $ab \in G$. Thus, a group cannot be written as the set-theoretic union of two proper subgroups. □

32. Show that a group G is the set-theoretic union of three proper subgroups if and only if G has, as a homomorphic image, a noncyclic group of order 4.

Proof. Suppose G is the set theoretic union of three proper subgroups L, M and N. That is, $G = L \cup M \cup N$. Note that a group is not an union of two proper subgroups, so there always exists an element which is not in the union of two.
First we claim that $L \cap M = L \cap N$. Let $u \in L \cap M$. If $u \notin N$, let $n \in N - (L \cup M)$. Then $un \notin N$ otherwise $u^{-1}un = n \in N$, a contradiction. Also, $un \notin L$, since $n \notin L$. Similarly, $un \notin M$. Therefore, $un \notin L \cup M \cup N = G$, a contradiction. This forces us that $L \cap M = L \cap N$. Moreover, with similar method, we can conclude that $L \cap M = L \cap N = M \cap N = L \cap M \cap N$.
Now we show that any product of x, y lying outside of L must lie in L itself. That is, if $x, y \notin L$, then $xy \in L$. Note that x and y each lie in at most one of M and N as $M \cap N \subset L$. So suppse $x \in M - (L \cup N)$ and $y \in N - (L \cup M)$. Then clearly $xy \notin M \cup N$ and hence $xy \in L$. WLOG, assume that $x, y \in M - (L \cup N)$. Let $z \in L - (M \cup N)$. Then $zx \notin L \cup M$ so that $zx \in N - (L \cup M)$. Now as $y \in M - (L \cup N)$, $(zx)y \notin M \cup N$, $zxy \in L$. Since $z \in L$, $z^{-1}zxy = xy \in L$. Moreover, we can change the role of L into M or N, as they play symmetrically.
Now we claim that $L \cap M \cap N$ is normal in G. Choose $x \in L \cap M \cap N$ and $g \in G$. If g lies in more than one of L, M and N, than $g \in L \cap M \cap N$ so that $gxg^{-1} \in L \cap M \cap N$. So we assume that g lies only at one of the L, M or N. Suppose $g \in L - (M \cup N)$, then $gx \notin M$, $g^{-1} \notin M$ so that $gxg^{-1} \in M$. Likewise, $gx \notin N$, $g^{-1} \notin N$ so that $gxg^{-1} \in N$. Thus $gxg^{-1} \in M \cap N = L \cap M \cap N$, so that $L \cap M \cap N$ is normal in G.
We now claim that $G/(L \cap M \cap N)$ is isomorphic to Klein-4 group. The nontrivial elements of $G/(L \cap M \cap N)$ corresponds to cosets represented by elements that lie exactly one of

L, M or N. If g and g' lies in L but not in $M \cup N$, then $g(L \cap M \cap N) = g'(L \cap M \cap N)$ since $gg'^{-1} \in (L \cap M \cap N)$. That is, we have exactly one coset corresponding to elements in L but not in $(L \cap M \cap N)$. So in total, there can be 4 elements in $G/(L \cap M \cap N)$ with each having order 2. So, $G/(L \cap M \cap N)$ is isomorphic to K_4.
Conversely, since K_4 is an union of three proper subgroups, if $G/K \simeq K_4 = L \cup M \cup N$, then the pullbacks of each L, M and N(for L, the pullback is L', $L'/K \simeq L$) are proper with union equal to G. □

33. Let p be a prime and let $\mathbb{Z}_p$ be the integers mod p under addition and multiplication. Let G be the group $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{Z}_p$ are such that $ad = bc = 1$. Let

$$C = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

and let $LF(2, p) = G/C$.
a) Find the order of $LP(2, p)$.

Solution. Note that $o(GL(2,p)) = (p^2 - 1)(p^2 - p)$. Thus $G = o(GL(2,p))/(p-1) = (p-1)p(p+1)$. Consequently, $o(LF(2,p)) = o(G)/o(C) = \dfrac{(p-1)p(p+1)}{2}$. □

b) Prove that $LF(2, p)$ is simple if $p \geq 5$.

Proof. Simplicity of Projective Linear Group for the case $n = 2$ is also know as Jordan-Moore Theorem. □

34. Prove that $LF(2, 5)$ is isomorphic to A_5, the alternating group of degree 5.

Proof. Every simple non-abelian group of order 60 is isomorphic to A_5. Calculating the Sylow subgroups of each, we can conclude the given fact easily. □

35. Let $G = LF(2, p)$; according to Problem 33, G is a simple group of order 168. Determine exactly how many 2-Sylow, 3-Sylow, and 7-Sylow subgroups there are in G.

Solution. There are 7 2-Sylow subgroups, 28 3-Sylow subgroups and 8 7-Sylow subgroups. □