Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 4, 2020

Problems in the Section 2.4. $\sim$ 2.5.

1. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?

Proof. Let $x, y \in H \cap K$. Since x, y are elements of both H and K, xy is also an element of both H and K. Hence, $xy \in H \cap K$. Further, x^{-1} is also in both H and K. This implies that $x^{-1} \in H \cap K$. Therefore, $H \cap K$ is a subgroup of G. Also, this same proof can be applied to intersection of any number of subgroups of G, either finite or infinite. □

2. Let G be a group such that the intersection of all its subgroups which are different from (e) is a subgroup different from (e). Prove that every element in G has finite order.

Proof. Suppose G has an element a of infinite order. Then (a) is an infinite cyclic subgroup of G. Now consider the intersection of every subgroup of (a), namely, $\bigcap_{n\in\mathbb{N}} (a^n)$. Any element in this subgroup must be of the form $a^m, m \in \mathbb{Z}$, where m is the multiple of all $n \in \mathbb{N}$. The only possible value of m is $m = 0$. Hence, $\bigcap_{n\in\mathbb{N}} (a^n) = (e)$, a contradiction. □

3. If G has no nontrivial subgroups, show that G must be finite of prime order.

Proof. First we show that G is of finite order. If not, then for $a \in G$, (a) is a subgroup of G. Suppose it is nontrivial, then we further consider $(a^2) \subset (a)$, which is a nontrivial subgroup of (a) and hence of G, a contradiction. Therefore, G is of finite order. Moreover, G must be cyclic as for any $a \neq e \in G$, (a) is a nontrivial subgroup of G and hence $(a) = G$. Now we assume that G is of non-prime order, say $o(G) = nm$. If $(a) = G$ then (a^n) is a nontrivial subgroup of G with order m, contradicting that G has no nontrivial subgroup. Thus, G must be finite of prime order. □

4. a) If H is a subgroup of G, and $a \in G$ let $aHa^{-1} = \{aha^{-1} : h \in H\}$. Show that aHa^{-1} is a subgroup of G.

Proof. Choose $x, y \in aHa^{-1}$. Then we can write $x = ah_1a^{-1}, y = ah_2a^{-1}$ for some $h_1, h_2 \in H$. Observe that

$$xy = (ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}, x^{-1} = ah_1^{-1}a^{-1} \in aHa^{-1}.$$

Now we have aHa^{-1} as a subgroup of G. □

b) If H is finite, what is $o(aHa^{-1})$?

Proof. Define a mapping $f : aHa^{-1} \to H$ by $f(x) = a^{-1}xa$. Then f is a bijection. Hence, $o(aHa^{-1}) = o(H)$. □

5. For a subgroup H of G define the left coset aH of H in G as the set of all elements of the form $ah, h \in H$. Show that there is a one-to-one correspondence between the set of all left cosets of H in G and the set of right cosets of H in G.

Proof. Let ϕ be a mapping between the set of left cosets of H and the set of right cosets of H, defined in a way that: $\phi(aH) = Ha^{-1}$. We show that ϕ is a bijection. Suppose $\phi(aH) = \phi(bH)$. Then $Ha^{-1} = Hb^{-1} \implies a^{-1}b \in H \implies aH = bH$. This shows that ϕ is injective. Further, for any right coset Hc, we have $\phi(c^{-1}H) = Hc$. This prove that ϕ is surjective. Therefore, ϕ is bijective and hence establishing an one-to-one correspondence between the set of all left cosets and the set of right cosets(of H in G). □

6. Write out all the right cosets of H in G where
a) $G = (a)$ is a cyclic group of order 10 and $H = (a^2)$ is the subgroup of G generated by a^2.

Solution. There are two right cosets, namely (a^2) and $(a^2)a$. □

b) G as in part a), $H = (a^5)$ is the subgroup of G generated by a^5.

Solution. There are five right cosets: (a^5), $(a^5)a$, $(a^5)a^2$, $(a^5)a^3$, $(a^5)a^4$. □

c) $G = A(S), S = \{x_1, x_2, x_3\}$, and $H = \{\sigma \in G : x_1\sigma = x_1\}$.

Solution. With the notation used in section 2.1, we can rewrite H as $H = \{id, \psi\phi\}$. There are three right cosets then: $H, H\psi = \{\psi, \phi\}, H\psi^2 = \{\psi^2, \psi^2\phi\}$. □

7. Write out all the left cosets of H in G for H in G as in parts a), b), c) of Problem 6.

Proof. We have the left cosets and right cosets same for the cases a) and b). For c), We have the three left cosets namely: $H, \psi H = \{\psi, \psi^2\phi\}, \psi^2 H = \{\psi^2, \phi\}$. □

8. Is every right coset of H in G a left coset of H in G in the groups of Problem 6?

Proof. No. Compare the list of left cosets and right cosets of H for the case c). □

9. Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subset H$ for all $G \in G$.

Proof. For the sake of contradiction, suppose there is an $g \in G$ and $h \in H$ such that $ghg^{-1} \notin H$. Note that $ghH = gH$ and hence by the given condition $H(gh) = Hg \implies ghg^{-1} \in H$. But this is clearly a contradiction. □

10. Let G be a group of integers under addition, H_n the subgroup consisting of all multiples of a fixed integer n in G. Determine the index of H_n in G and write out all the right cosets of H_n in G.

Proof. There are n distinct right cosets of H_n in G:

$$H_n,\ , H_n + 1,\ H_n + 2, \cdots,\ H_n + (n-1).$$

Hence the index of H_n in G is n. □

11. In Problem 10, what is $H_n \cap H_m$?

Proof. Elements in $H_n \cap H_m$ must form a set of all multiples of n and m. That is, the set of multiples of $\text{lcm}(n, m)$, least common multiple of n and m. Clearly, every multiples of $\text{lcm}(n, m)$ is in both H_n and H_m. Therefore, $H_n \cap H_m = H_{\text{lcm}(n,m)}$. □

12. If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index in G. Can you find an upper bound for the index of $H \cap K$ in G?

Proof. Since $a(H \cap K) = aH \cap aK$ for all $a \in G$ and choices for each aH and aK are finite, so does the number of $a(H \cap K)$. Thus, $H \cap K$ is of finite index in G. From our assertion, it can be found that the multiple of indices of H and K is an upper bound for the index of $H \cap K$ in G. □

13. If $a \in G$, define $N(a) = \{x \in G : xa = ax\}$. Show that $N(a)$ is a subgroup of G. $N(a)$ is usually called the Normalizer or Centralizer of a in G.

Proof. For any $x, y \in N(a)$, $(xy)a = x(ya) = x(ay) = (xa)y = a(xy)$. Hence, $xy \in N(a)$. Also, $xa = ax \implies a = x^{-1}ax \implies ax^{-1} = x^{-1}a$, implying $x^{-1} \in N(a)$. Therefore, $N(a)$ is a subgroup of G. □

14. If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G : xh = hx \text{ all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

Proof. For any $x, y \in C(H), h \in H$, $(xy)h = h(ya) = x(hy) = (xh)y = h(xy)$. Hence, $xy \in C(H)$. Also, $xh = hx \implies h = x^{-1}hx \implies hx^{-1} = x^{-1}h$, implying $x^{-1} \in C(H)$. Therefore, $C(H)$ is a subgroup of G. □

15. The Center Z of a group is defined by $Z = \{z \in G : zx = xz \text{ all } x \in G\}$. Prove that Z is a subgroup of G. Can you recognize Z as $C(T)$ for some subgroup T of G?

Proof. This is a special case of Problem 14. Set $H = G$. That is, $Z = C(G)$. □

16. If H a subgroup of G, let $N(H) = \{a \in G : aHa^{-1} = H\}$. Prove that
a) $N(H)$ is a subgroup of G.

Proof. For any $x, y \in N(H)$, $(xy)H(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$ implying $xy \in N(H)$. Further, $x^{-1}Hx = x^{-1}(xHx^{-1})x = H$ implying $x^{-1} \in N(H)$. Hence, $N(H)$ is a subgroup of G. □

b) $N(H) \supset H$.

Proof. Note that for all $h \in H$, $hHh^{-1} = H$ trivially. Hence, $H \subset N(H)$. □

17. Give an example of a group G and a subgroup H such that $N(H) \neq C(H)$. Is there any containing relation between $N(H)$ and $C(H)$?

Proof. Consider the group of quaternions, $G = \{\pm 1, \pm i \pm j, \pm k\}$, $ij = k$, $jk = i$, $ki = j$, $i^2 = j^2 = k^2 = -1$. Let $H = \{\pm 1, \pm i\}$. By some calculations, we see that $N(H) = G$, $C(H) = H$. Therefore, $N(H) \neq C(H)$. Moreover, in general, if $x \in C(H)$, $xhx^{-1} = h$ for all $h \in H$ implying $xHx^{-1} = H$. Thus, $x \in N(H)$ and hence, $C(H) \subset N(H)$. □

18. If H is a subgroup of G let

$$N = \bigcap_{x \in G} xHx^{-1}.$$

Prove that N is a subgroup of G such that $aNa^{-1} = N$ for all $a \in G$.

Proof. Note that for all $a \in G$, every element $y \in G$ is expressible in the form $y = ax$ for some unique $x \in G$.Keeping this in mind, choose $n \in N$. Then, $n \in xHx^{-1}$ for any $x \in G$. Hence, $ana^{-1} \in (ax)H(ax)^{-1} = yHy^{-1}$, for some $y \in G$. Since x arbitrary and each y corresponding to x would be distinct by the choices of x, $ana^{-1} \in xHx^{-1}$ for all $x \in G$. Thus, $aNa^{-1} \subset N$. Similarly, $N \subset aNa^{-1}$. Therefore, $aNa^{-1} = N$. □

19. If H is a subgroup of finite index in G, prove that there is only a finite number of distinct subgroups in G of the form aHa^{-1}.

Proof. Suppose $aH = bH$. Then $Ha^{-1} = Hb^{-1}$ implying $aHa^{-1} = bHb^{-1}$. Since H is of finite index, there is only a finite number of distinct subgroups of the form aHa^{-1} in G. □

20. If H is of finite index in G prove that there is a subgroup N of G, contained in H, and of finite index in G such that $aNa^{-1} = N$ for all $a \in G$. Can you give an upper bound for the index of this N in G?

Proof. Let $N = \bigcap_{x \in G} xHx^{-1}$. From the definition, N is clearly contained in H. By Problem 18, N is a group satisfying $aNa^{-1} = N$ for all $a \in G$. Moreover, by Problem 19, there are finitely many distinct subgroups of G of the form xHx^{-1}. Thus, N is an intersection of finitely many subgroup of G. Moreover, since $o(H) = o(xHx^{-1})$ and H is of finite index in G, so does every xHx^{-1}. Now, by Problem 12, since $N = \bigcap_{x \in G} xHx^{-1}$, intersection of finitely many subgroups of finite indices, N is of finite index in G. To find an upper bound for the index of N, let k denote the number of distinct subgroups of the form xHx^{-1} and n denote the index of H in G. By applying the Problem 12 again, we see that n^k is an upper bound for index of N in G. □

21. Let the mapping τ_{ab} for a, b real numbers, map the reals into the reals by the rule $\tau_{ab} : x \to ax + b$. Let $G = \{\tau_{ab} : a \neq 0\}$. Prove that G is a group under the composition of mappings. Find the formula for $\tau_{ab}\tau_{cd}$.

Proof. Let $\tau_{ab}, \tau_{cd} \in G$. Then $\tau_{ab} \cdot \tau_{cd} = a(cx + d) + b = acx + (ad + b) = \tau_{(ac)(ad+b)} \in G$. We have the identity element $\tau_{10} = x$. For the inverse element(of τ_{ab}), take $\tau_{\frac{1}{a}\frac{-b}{a}}$. Hence, G is a group under composition of mappings. □

22. In Problem 21, let $H = \{\tau_{ab} \in G : a \in \mathbb{Q}\}$. Show that H is a subgroup of G. List all the right cosets of H in G, and all the left cosets of H in G. From this show that every left coset of H in G is right coset of H in G.

Proof. Note that multiple of two rationals is rational and inverse of rational is rational. Keeping this in mind and applying the method used in Problem 21, it is easy to see that H is a subgroup of G. List of all the right cosets can be expressed as $H\tau_{rs}$, where $0 \neq r, s \in \mathbb{R}$. Similarly, for left cosets, $\tau_{rs}H$. In fact, every left coset and right coset is same, since for any $t = h\tau_{rs}, h \in H, h = \tau_{ab}$,

$$t = \tau_{ab} \cdot \tau_{rs} = (ar)x + (as + b) = \tau_{rs} \cdot \tau_{r, \frac{(a-1)s+b}{d}} \in \tau_{rs}H.$$

This implies $H\tau_{rs} = \tau_{rs}H$ for all $r \neq 0, s \in \mathbb{R}$. □

23. In the group G of Problem 21, let $N = \{\tau_{1b} \in G\}$. Prove
a) N is a subgroup of G.

Proof. For any $\tau_{1a}, \tau_{1b} \in N$, $\tau_{1a}\tau_{1b} = \tau_{1,b+a} \in N$. Moreover, $\tau_{1,-a}$ is the inverse element for each $\tau_{1a} \in N$. Hence N is a subgroup of G. □

b) If $a \in G$, $n \in N$, then $ana^{-1} \in N$.

Proof. Note that for any $\tau_{ab} \in G$, $\tau_{1c} \in N$,

$$\tau_{ab} \cdot \tau_{1c} \cdot \tau_{\frac{1}{a}, \frac{-b}{a}} = \tau_{1,ac} \in N.$$

□

24. Let G be a finite group whose order is not divisible by 3. Suppose that $(ab)^3 = a^3b^3$ for all $a, b \in G$. Prove that G must be abelian.

Proof. Consider a mapping $\phi : G \to G$ defined as $\phi(x) = x^3$. Then ϕ is an homomorphism and injective since $x^3 = e$ holds only for $x = e$, otherwise x has order divisible by 3. Therefore, by Pigeonhole Principle, ϕ is a bijetion. Hence, every element in G can be expressed uniquely as a cube of an element in G. Now we see that

$$(ab)^4 = ((ab)^2)^2 = (b^2a^2)^2 = (a^2)^2(b^2)^2 = a^4b^4$$

implying

$$(ab)^4 = a^4b^4 \implies (ba)^3 = a^3b^3 \implies b^3a^3 = a^3b^3$$

for all $a, b \in G$. Now for any $x, y \in G$ we can set $x = a^3, y = b^3$. Then we see that G is abelian. □

25. Let G be an abelian group and suppose that G has elements of order m and n respectively. Prove that G has an element whose order is the least common multiple of m and n.

Proof. First, we prove the case when $\gcd(m, n) = 1$, i.e. m, n are relatively prime. Let a, b be the elements of G with order m, n respectively. Clearly,

$$(ab)^{mn} = (a^m)^n(b^n)^m = e.$$

Let k be the order of ab. Then we know that $k \leq mn$. Moreover,

$$\begin{aligned} e = (ab)^{km} = b^{km} &\implies n|km \implies n|k, \\ e = (ab)^{kn} = a^{kn} &\implies m|kn \implies m|k \end{aligned}$$

implying $\text{lcm}(m, n) = mn|k \implies k = mn$. Therefore, if $\gcd(m, n) = 1$, there exists an element of order $\text{lcm}(m, n) = mn$. Now, suppose given m, n are not relatively prime. Say $m = \prod_i p_i^{m_i}, n = \prod_i p_i^{m_i}$ where p_i are distinct primes. Note that $\text{lcm}(m, n) = \prod_i p_i^{\max(m_i, n_i)}$. Now we define

$$m' = \prod_{i \in M} p_i^{m_i}, \quad n' = \prod_{i \in N} p_i^{n_i}$$

where $M = \{i : m_i \geq n_i\}$, $N = \{i : m_i < n_i\}$. We see that $a' = a^{m/m'}$ has order of m' and $b' = b^{n/n'}$ has order of n' and $(m', n') = 1$. Hence, G has an element of order $m'n' = \text{lcm}(m, n)$. □

26. If an abelian group has subgroups of orders m and n, respectively, then show that it has a subgroup whose order is the least common multiple of m and n.

Proof. We rather prove this problem in more sophisticated manner. That is, we assume the following lemma: If a finite abelian group G exists and d is a positive integer such that d divides $o(G)$, then there is a subgroup of G of order d. This comes from the fact that every finite abelian group can be expressed as a direct product of sylow subgroups, expressing d into product of power of primes and taking appropriate subgroups in the direct product. Now, we set H and K be the subgroup of G with orders m and n respectively. Then we have

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

Note that by Lagrange's theorem, $o(H \cap K)$ divides both $o(H) = m, o(K) = n$. Hence, $\gcd(m, n)|o(H \cap K)$. Moreover, $\text{lcm}(m, n)|o(HK)$ from the above identity. Since HK is abelian, there exists a subgroup of HK(hence of G) of order $\text{lcm}(m, n)$. □

27. Prove that any subgroup of a cyclic group is itself a cyclic group.

Proof. Let $G = (a)$ for some $a \in G$. Let H be a subgroup of G. Since G is cyclic, H constitutes elements of the form a^k. Let k be the smallest positive integer such that $a^k \in H$. We claim that $H = (a^k)$. Assume $a^m \in H$. Then there exists integers q, r such that $m = qk + r$, $0 \leq r < k$. Since $a^{m-qk} \in H, a^r \in H$. But this contradicts the definition of k. Thus, every elements of H is of the form $(a^k)^q$, where q is an integer. Therefore, H is a cyclic group. □

28. How many generators does a cyclic group of order n have?

Proof. We claim that there are $\phi(n)$ generators for a cyclic group of order n. Here, ϕ is the euler totient function. Let $G = (a)$. Suppose we consider a^k, $k|n$. Then clearly a^k has order strictly less than n so that it cannot generate G. Now we consider a^k where $(k, n) = 1$. $(a^k)^n = e$ is trivial. If t is the order of a^k, using the fact that there exists integers μ, λ such that $k\mu + n\lambda = 1$,

$$e = (a^k)^t = a^{kt\mu} = a^{t(1-n\lambda)} = a^t \implies n|t \implies t = n,$$

implying the order of a^k is n. Therefore, there are exactly $\phi(n)$ generators for a cyclic group of order n. □

29. Show that U_8 is not a cyclic group.

Proof. It is easy to see that $U_8 = \{1, 3, 5, 7\}$. But $1 \equiv 1 \mod 8$, $3^2 \equiv 1 \mod 8$, $5^2 \equiv 1 \mod 8$, $7^2 \equiv 1 \mod 8$ implying none of the elements of U_8 can generate the whole set. □

30. Show that U_9 is a cyclic group. What are all its generators?

Proof. Note that $U_9 = \{1, 2, 4, 5, 7, 8\}$. $5, 8$ are the generators of the U_9. □

31. Show that U_{17} is a cyclic group. What are all its generators?

Proof. Note that $U_{17} = \{1, 2, \cdots, 16\}$. There are 8 generators: $3, 5, 6, 7, 10, 11, 12, 14$. □

32. Show that U_{18} is a cyclic group.

Proof. Note that $U_{18} = \{1, 5, 7, 11, 13, 17\}$. $5, 11$ are the generators of U_{18}. □

33. Show that U_{20} is not a cyclic group.

Proof. Note that $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. But

$$1 \equiv 1,\ 3^4 \equiv 1,\ 7^4 \equiv 1,\ 9^2 \equiv 1,$$
$$11^2 \equiv 1,\ 13^4 \equiv 1,\ 17^4 \equiv 1,\ 19^2 \equiv 1$$

under modulo 20. Hence, U_{20} is not a cyclic group. □

34. Show that both U_{25} and U_{27} are cyclic groups.

Proof. For both U_{25} and U_{27}, 2 is a generator of each. Hence, both are cyclic. □

35. Hazard a guess at what all the n such that U_n is cyclic are.

Proof. We prove that U_n is cyclic if and only if $n = 1, 2, 4, p^k, 2p^k$ where p is an odd prime. First, we state a famous lemma known as Chinese Remainder Theorem:

Lemma 1. If $n = p_1^{q_1} p_2^{q_2} \cdots p_k^{q_k}$ be the prime factorization of n, then

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{q_1}\mathbb{Z} \times \mathbb{Z}/p_2^{q_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{q_k}\mathbb{Z}. \tag{1}$$

From this, we have that:

$$U_n \simeq U_{p_1^{q_1}} \times U_{p_2^{q_2}} \times \cdots \times U_{p_k^{q_k}}. \tag{2}$$

We introduce another lemma:

Lemma 2. For an abelian G, if $G \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, then G is cyclic if and only if $\gcd(m, n) = 1$.

Suppose $n = 1$. Then the group U_1 is trivially cyclic. If $n = 2$, then $U_2 = \{1\}$ and hence, cyclic. If $n = 4$, then $U_4 = \{1, 3\}$. Since it is group of order 2, so it is cyclic. Now we investigate the case for n is divisible by p, q where p, q are distinct odd primes. Note that the order of U_{p^k} is $\phi(p^k) = p^{k-1}(p-1)$. As we said that p, q divides n, n is expressible as $n = p^k q^s \cdots$ and consequently by equation (2), $U_n \simeq U_{p^k} \times U_{q^s} \times \cdots$. For we assume that U_{p^k} and U_{q^s} are cyclic, since $p-1$ and $q-1$ are even, $\gcd(\phi(p^k), \phi(q^s)) > 1$ and hence G cannot be cyclic. Also, if we change $q = 4$ in our previous argument, we have the same result. So if we prove that U_{p^k} is cyclic for every odd prime p and positive integer $k > 1$, the possible substitute for U_n to be cyclic are $1, 2, 4, p^k, 2p^k$. Our task is now to prove U_{p^k} is a cyclic group.

We first prove that U_p is cyclic. Note that U_p is isomorphic to multiplicative subgroup of finite field $\mathbb{Z}_p$. Then consider a polynomial $x^d = 1$, where d is a positive integer. Note that in a field, number of elements satisfying $x^d = 1$ is at most d. Therefore, applying the argument of the Problem 38, we have that U_p is cyclic. Now we show that U_{p^2} is cyclic. We introduce a new lemma:

Lemma 3. If g is a generator for U_p and let k be an integer such that $p \nmid k$, then either g or $g + kp$ generates U_{p^2}.

Proof. Since the order of U_{p^2} is $\phi(p^2) = p(p-1)$, $g, g + kp$ have order dividing $p(p-1)$. It is must that order of both g and $g + kp$ be multiples of $p - 1$ otherwise they cannot generate U_p. So, the only possible choices are $p(p-1)$ and $p - 1$. We claim that at least one of g and $g + kp$ has order $p(p-1)$. For the sake of contradiction, assume they both have order of $p - 1$. At then, we have

$$1 \equiv (g + kp)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} g^{p-2} kp + \binom{p-1}{2} g^{p-3} (kp)^2 + \cdots \pmod{p^2}$$

Note that $g^{p-1} \equiv 1 \pmod{p}$ by Fermat's little Theorem. Then the above equation can be reduced into

$$1 \equiv 1 + (p-1) g^{p-2} kp \pmod{p^2} \iff 0 \equiv (p-1) g^{p-2} kp \pmod{p^2}.$$

But since $p \nmid (p-1) g^{p-2} k$, this is a contradiction. Hence the lemma is proved. □

Now we have that U_{p^2} as a cyclic group. We shall further prove that U_{p^k} is cyclic for all $k > 2$. Again, we introduce another lemma:

Lemma 4. Let p be an odd prime and $a \geq 1$. Then,

$$(1 + kp)^{p^a} \equiv 1 + kp^{a+1} \pmod{p^{a+2}}$$

Proof. If $a = 1$, we see that

$$(1 + kp)^p \equiv 1 + \binom{p}{1} kp + \cdots \pmod{p^3} \iff (1 + kp)^p = 1 + kp^2 + n_1 p^3$$

for some $n_1 \in \mathbb{Z}$. Suppose we assume that the statement holds for some $a \geq 1$, so

$$(1 + kp)^{p^{a+1}} = ((1 + kp)^{p^a})^p = (1 + kp^{a+1} + np^{a+2})^p$$

for some $n \in \mathbb{Z}$. Now we think the trinomial expansion of $(1 + kp^{a+1} + np^{a+2})^p$:

$$\sum_{i+j+k=p} \binom{p}{i, j, k} (1)^i (kp^{a+1})^j (np^{a+2})^k.$$

We have several cases to consider. On summarzing, we result out that 1 and the term involving no factors of np^{a+2} and only one kp^{a+1}, that is, 1 and

$$\binom{p}{p-1, 1, 0} kp^{a+1} = kp^{a+2},$$

are the only terms in the trinomial expansion which are not divisible by p^{a+3}. Therefore, we have

$$(1 + kp)^{p^{a+1}} = ((1 + kp)^{p^a})^p = 1 + kp^{a+2} + mp^{a+3}$$

for some $m \in \mathbb{Z}$, completing our induction procedure. □

Now suppose we assume that g is the generator of U_{p^2}. Since g is of order $p(p-1)$ in modulo p^2, it has order $p^a(p-1)$, $0 \leq a < m$ for modulo p^m. All the possibilities divide $p^{m-2}(p-1)$ except for $p^{m-1}(p-1)$, hence it is enough to show that $g^{p^{m-2}(p-1)} \not\equiv 1 \mod p^m$. Since g generates U_{p^2}, we have $g^{p-1} = 1 + kp$ for $p \nmid k$. Now by Lemma 4,

$$g^{p^{m-2}(p-1)} = (g^{p-1})^{p^{m-2}} = (1 + kp)^{p^{m-2}} = 1 + kp^{m-1} + np^m$$

for some $n \in \mathbb{Z}$, showing that $g^{p^{m-2}(p-1)} \not\equiv 1 \mod p^m$. Thus, the only possibility for the order of g modulo p^m is $p^{m-1}(p-1) = \phi(p^m)$, g generates U_{p^m}. Hence, we have proved that U_{p^k} is cyclic for all odd prime p.

Let's get back to the beginning. Since we have shown that U_{p^k} is cyclic, U_n is cyclic if and only if $n = 1, 2, 4, p^k, 2p^k$. Our proof is now done. □

36. If $a \in G$ and $a^m = e$, prove that $o(a) \mid m$.

Proof. For the sake of contradiction, assume that $o(a) = n \nmid m$. That is, $m = nq + r$ for some integers q, r such that $0 \leq r < n$. Since $a^m = e$,

$$e = a^m = a^{nq+r} = a^r$$

implying n is not the smallest (positive) integer satisfying $a^n = e$, contradicting the definition of n. Hence, $o(a) \mid m$. □

37. If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for some $a, b \in G$, find $o(b)$.

Proof. Note that

$$\begin{aligned} b^4 &= aba^{-1} \cdot aba^{-1} = ab^2a^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2} \\ &\implies b^8 = a^2ba^{-2} \cdot a^2ba^{-2} = a^2b^2a^{-2} = a^2(aba^{-1})a^{-2} = a^3ba^{-3} \\ &\implies b^{16} = a^3ba^{-3} \cdot a^3ba^{-3} = a^3b^2a^{-3} = a^3(aba^{-1})a^{-3} = a^4ba^{-4} \\ &\implies b^{32} = a^4ba^{-4} \cdot a^4ba^{-4} = a^4b^2a^{-4} = a^4(aba^{-1})a^{-4} = a^5ba^{-5} = b \implies b^{31} = e. \end{aligned}$$

Since 31 is prime, unless b is an identity, $o(b) = 31$. □

38. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n. Prove that G must be a cyclic group.

Proof. Let us define a set A_d for every $d \in \mathbb{N}$ as

$$A_d = \{x \in G : x^d = e, x \text{ is of order } d\}.$$

By the given condition, we have $o(A_d) \leq \phi(d)$, where ϕ is the euler totient function. Nevertheless,

$$n = \sum_{d|n} o(A_d) \leq \sum_{d|n} \phi(d) = n,$$

implying $A_n \neq \emptyset$. Thus, there exists an element $g \in A_n \iff G = (g)$. □

39. Let G be a group and A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A, b \in B$. Prove
a) The relation so defined is an equivalence relation.

Proof. We have $x = exe = x$, so that $x \sim x$. Also, if $x \sim y$, equivalently $y = axb$ for some $a \in A, b \in B$, so $x = a^{-1}yb^{-1}$, hence $y \sim x$. Now suppose $x \sim y$ and $y \sim z$. Then, $y = axb, z = a'yb'$ for some $a, a' \in A, b, b' \in B$. Consequently, $z = a'axbb' = (a'a)x(bb')$, implying $x \sim z$. Hence, the given relation is an equivalence relation. □

b) The equivalence class of x is $AxB = \{axb : a \in A,\ b \in B\}$

Proof. Since given set AxB is set of all the elements of the form axb, it is trivial that equivalence class of x is AxB itself. □

40. If G is a group, show that the number of elements in the double coset AxB is

$$\frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

Proof. Let us define a mapping $\phi : AxB \to AxBx^{-1}$ by $\phi(axb) = axbx^{-1}$. By the definition itself, this mapping is clearly onto. Moreover, if $axbx^{-1} = a'xb'x^{-1}$, then $axb = a'xb'$ implying $a = a', b = b'$. Thus, ϕ is one-one, hence, bijective. Now, we have

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

□

41. If G is a finite group and A is a subgroup of G such that all double cosets AxA have the same number of elements, show that $gAg^{-1} = A$ for all $g \in G$.

Proof. Note that $o(AeA) = o(A)$. Also from the Problem 40,

$$o(AxA) = \frac{o(A)o(A)}{o(A \cap xAx^{-1})} = \frac{o(A)^2}{o(A \cap xAx^{-1})}.$$

Since by the hypothesis, $o(AxA) = o(A)$ for all $x \in G$, we have that $o(A \cap xAx^{-1}) = o(A)$. Also, $A \cap xAx^{-1} \subset A$. This implies that $A \subset xAx^{-1}$. By changing $x = g^{-1}$, we also have $A \subset g^{-1}Ag \implies gAg^{-1} \subset A$. Since g was arbitrary, $gAg^{-1} = A$ for all $g \in G$. □