

Answer key No.2 to selected homework problems: Math. 110B

7.6

1. $aK = K$ means $ae = k \in K$; so, $a \in K$. Conversely, if $a \in K$, then $ak \in K$ for all $k \in K$ because K is a subgroup. This shows $aK \subset K$. Pick any $k \in K$, then $k = ek = (aa^{-1})k = a(a^{-1}k) \in aK$, because K is subgroup. Thus $K \subset aK$. This combined the earlier reverse inclusion shows that $K = aK$. \square
2. (a) (1) Every left coset aK is a subset of G ; so, $\bigcup_a aK \subset G$. For each $g \in G$, $g = ge \in gK$; so, $G \supset \bigcup_a aK$.
 (2) Define $f : K \rightarrow aK$ by $f(k) = ak$. To show f is injective, assume that $f(x) = f(y)$. Then we need to show that $x = y$. $f(x) = f(y)$ implies $ax = ay$; then, by left-cancellation, we find $x = y$. $x \in aK$ implies $x = ak$ for $k \in K$; so, $x = f(k)$; therefore, f is surjective. Thus f is a bijection. In particular $|aK| = |K|$ if $|K|$ is finite.
- (b) We need to show that there are only two possibilities: $aK = bK$ or $aK \cap bK = \emptyset$. Thus we need to show: $aK \cap bK \neq \emptyset \Rightarrow aK = bK$. Pick $x = ak = bk'$ in the intersection. Then $b^{-1}a = k'k^{-1} \in K$. Thus $a^{-1}bk \in K$ for all $k \in K$; in particular, $bk = ebk = (aa^{-1})bk = a(a^{-1}bk) \in aK$; thus $aK \subset bK$. Interchanging the role of a and b in the above argument, we find the reverse inclusion $aK \supset bK$; so, $aK = bK$ as desired. We are going to prove that G is a union of left cosets c_1K, c_2K, \dots without overlapping (such a union is written as $G = c_1K \sqcup c_2K \sqcup \dots \sqcup c_mK$ (here $m = [G : K]$) using the disjoint union symbol " \sqcup ". Now start with $K = eK$, and write $c_1 = e$. Pick c_2 outside $c_1K = K$ if any. If there is none, we have $G = K$. Otherwise, $c_1K \neq c_2K$ because c_2 is not in c_1K ; so, we have $c_1K \cap c_2K = \emptyset$. Suppose we have found c_1, \dots, c_n so that $c_iK \cap c_jK = \emptyset$ for any pairs (i, j) with $i \neq j$. By induction on n , we try to find c_{n+1} with the same disjointness property. Take $c = c_{n+1}$ outside $c_1K \cup c_2K \cup \dots \cup c_nK$ if any. If there is none, we have $G = c_1K \sqcup c_2K \sqcup \dots \sqcup c_nK$; so, we are done, getting a disjoint union expression of G by left cosets. Otherwise, we have $c_jK \neq cK$ for all $j = 1, 2, \dots, n$ because $c \notin c_jK$. Thus only possibility is to have $cK \cap c_jK = \emptyset$; so, by induction on n , we can keep going. Since G is a finite group, the sequence c_1, c_2, \dots has to end at some point (exhausting all elements), so at the end, we find the disjoint union expression. Then $|G| = \sum_{j=1}^m |c_jK|$. By (a), $|c_jK| = |K|$, we find $|G| = m|K|$; so, we are done.
- (c) By (b), the number of left cosets is $|G|/|K|$. The number of right cosets is also $|G|/|K|$ by Lagrange theorem; so, they are equal to each other.
4.
 - Note that $\langle e \rangle$ is made of single element e . Then $xex^{-1} = xx^{-1} = e$; so, $x\langle e \rangle x^{-1} \subset \langle e \rangle$; so, by Theorem 7.34 (3), $\langle e \rangle$ is normal.
 - Since G is a group $xGy \subset G$; in particular, $xGx^{-1} \subset G$; so, again by Theorem 7.34 (3), it is normal.
5. (a) Hint: Compute the product of two upper triangular matrices to show it is again upper triangular. Also inverse of an upper triangular matrix is again upper triangular by computation.

9. By the existence of $b \in G$ with $Na = bN$ for each $a \in G$, we find $a = ea = bn$ for $n \in N$. Then $bN \cap aN \ni a$. As seen in Exercise 2, this implies $aN = bN$. Thus $Na = bN = aN$ for every $a \in N$; so, N is normal (see Definition in page 211).
14. Follow the hint of the exercise. By the multiplication table in page 167, the center of D_4 is made of r_0 and r_2 ; so, $N = \{h, v, r_2, r_0\}$ is a commutative group. Thus every subgroup of N is normal; in particular, $M = \{v, r_0\}$ is normal in N . To show that N is normal in G , we have $G = D_4 = N \sqcup r_1N$ (by Exercise 2). Again by the multiplication table, $r_1hr_1^{-1} = r_1hr_3 = v$ and $r_1vr_1^{-1} = h$; so, $r_1Nr_1^{-1} = N$. For all $x = r_1n \in r_1N$, $xNx^{-1} = r_1nNn^{-1}r_1^{-1}$ (see Corollary 7.6). Since $nNn^{-1} = N$ because N is a subgroup and $n \in N$; so, $xNx^{-1} = N$. This shows that N is a normal subgroup of D_4 . By $r_1vr_1^{-1} = h$, $r_1Mr_1^{-1} \neq M$; so, M is not normal in $G = D_4$.
15. Pick $k \in K$. Then $f(xkx^{-1}) = f(x)k(k)f(x)^{-1} = f(x)e_H f(x)^{-1} = f(x)f(x)^{-1} = e_H$ (see Theorem 7.19 (2)). Thus $xkx^{-1} \in K$; so, $xKx^{-1} \subset K$. By Theorem 7.34 (3), K is normal in G .
16. Pick $x \in K \cap N$. Then $gKg^{-1} \in gKg^{-1} = K$ and $gNg^{-1} \in gNg^{-1} = N$. Thus $gKg^{-1} \in K \cap N$. This shows $g(K \cap N)g^{-1} \subset K \cap N$; so, by Theorem 7.34 (3), $K \cap N$ is normal in G .
18. (a) Since N is normal in G , for every $g \in G$, $gng^{-1} = n_1$ for $n_1 \in N$. Take $nk, n'k' \in NK$. We need to show that $nk n'k' \in NK$ and $(nk)^{-1} \in NK$, because $e = ee \in NK$. We compute $nk n'k' = nk n'k^{-1}kk' = n(knk^{-1})kk' \in NK$ because $knk^{-1} \in N$. Similarly $(nk)^{-1} = k^{-1}n^{-1} = k^{-1}n^{-1}kk^{-1} \in NK$, because $k^{-1}n^{-1}k \in N$.
- (b) Since $g(nk)g^{-1} = gng^{-1}gkg^{-1} \in gNg^{-1}gKg^{-1} = NK$, we find, for every $g \in G$, $g(NK)g^{-1} \subset NK$; so, by Theorem 7.34 (3), NK is normal.
20. If $a \in N$, then $aN = Na$ because N is a subgroup. If $a \notin N$, we have $G = N \sqcup aN = N \sqcup Nb$ for some b , we find $aN = G - N = Nb$; so, by definition, N is normal.
21. For every $h \in H$, we find $g \in G$ such that $f(g) = h$. Then for each $n \in N$, we see that

$$hf(n)h^{-1} = f(g)f(n)f(g)^{-1} \stackrel{7.19}{=} f(g)f(n)f(g^{-1})$$

$$\stackrel{f:\text{hom}}{=} f(gng^{-1}) \in f(gNg^{-1}) \stackrel{gNg^{-1}=N}{\subset} f(N).$$

This shows that $hf(N)h^{-1} \subset f(N)$; so, by Theorem 7.34 (3), $f(N)$ is normal.

25. • Suppose first that for any $a, b \in G$, $ab \in N \Leftrightarrow ba \in N$. If $gNg^{-1} \in N$, applying the above identity for $a = gx$ and $b = g^{-1}$, we find $x = g^{-1}gx \in N$. But $gNg^{-1} \in N \Leftrightarrow x \in g^{-1}Ng$. So we get $x \in g^{-1}Ng \Rightarrow x \in N$. This shows $g^{-1}Ng \subset N$. Then by Theorem 7.34 (2), N is normal.
- Now suppose conversely that N is normal. If $ab \in N$, then $ba = a^{-1}(ab)a \in a^{-1}Na = N$. If $ba \in N$, then $ab = b^{-1}(ba)b \in b^{-1}Nb = N$; so, $ab \in N \Leftrightarrow ba \in N$.

7.7

1. Hint: Either make a multiplication table of S_3 to verify the subgroup is normal, or use the isomorphism $D_3 \cong S_3$ and the subgroup corresponds to the subgroup of rotations of D_3 . Then use the fact the flip-rotation-flip is again a rotation.
8. Because $(xN)(xN) = x^2N = N$. Thus the order of $xN \leq 2$. If xN is not the identity, the order is bigger than 1; so, it has to be 2.
11. (a) Writing the permutation interchanging exactly two numbers a, b as (ab) , the group V is made up of the identity, $(12)(34) = (34)(12)$, $(13)(24) = (24)(13)$ and $(14)(23) = (23)(14)$. In other words, V is made up of the identity and all products $(ab)(cd)$ with $\{1, 2, 3, 4\} = \{a, b\} \sqcup \{c, d\}$. For any permutation σ taking a to $\sigma(a)$ and b to $\sigma(b)$, we see

$$\sigma(a) \xrightarrow{\sigma^{-1}} a \xrightarrow{(ab)} b \xrightarrow{\sigma} \sigma(b).$$

Then $\sigma(ab)\sigma^{-1} = (\sigma(a)\sigma(b))$ and

$$\sigma(ab)(cd)\sigma^{-1} = (\sigma(ab)\sigma^{-1}\sigma(cd)\sigma^{-1}) = (\sigma(a)\sigma(b)(\sigma(c)\sigma(d))).$$

Thus $\sigma V \sigma^{-1} \subset V$; so, by Theorem 7.34 (3), we find that V is normal.

(b) Just a lot of computation; do it yourself!

12. Easy! because xN is just a pair $\{x, -x\}$; so, send xN to its absolute value $|x|$, and show this function is an isomorphism.
15. (b) Compute the order of $\frac{1}{n} + \mathbb{Z}$.
18. Define $f : G \rightarrow G/M \times G/N$ by $f(x) = (xM, xN)$. If $f(x) = f(y)$, then $xM = yM$ and $xN = yN$; so,

$$y^{-1}x \in M \cap N = \{e\} \Rightarrow y^{-1}x = e \Rightarrow x = y.$$

Thus f is injective, and hence $G \cong \text{Im}(f) \subset (G/M \times G/N)$.

21. Let $x \in Z(G)$ be an element with greatest order. Write simply $Z = Z(G)$. We may assume that $p \geq q$. Then $|x| \mid pq$. Thus there is three possibilities
 - $|x| = pq \Rightarrow Z(G) = G$, because $\langle x \rangle$ is a cyclic subgroup of order pq ;
 - $|x| = 1 \Rightarrow Z(G) = \{e\}$;
 - $|x| = p$. If $Z \neq G$, then $p \geq |\langle x \rangle| \mid pq$ implies that $Z = \langle x \rangle$, which is a cyclic group of order p (Theorem 7.28). Then we have $G/Z(G)$ is of order a prime q ; so, it is cyclic. Take a generator $yZ \in G/Z$. If $y^q \in Z$ is not an identity. Then y^q generates Z because it any non-identity of a group of prime order is a generator. Thus G is cyclic of order pq and $Z = G$, a contradiction to the fact that $|x|$ has greatest order in Z . Thus $y^q = e$. Since $G = Z \sqcup yZ \sqcup \dots \sqcup y^{q-1}Z$ and y commutes with x (because x is in the center), $N = \langle y \rangle$ is a normal subgroup. $N \cap Z = \{e\}$ by our choice of y . Then by Exercise 18, G is isomorphic to a subgroup of $G/Z \times G/N$, which is an abelian group, because G/N has order prime p (Theorem 7.28). Thus $Z(G) = G$, a contradiction; so, this case never occur.

22. Let n_1, \dots, n_r be generators of N , and let q_1N, \dots, q_mN be generators of G/N . Since G is a union of xN for $x \in G$, and xN can be written as a product of q_j , $x = qn$ for a product q of q_j 's and $n \in N$. Since n is a product of n_i , we find that every x is a product of q_j and n_i ; so, G is generated by $\{q_1, \dots, q_m, n_1, \dots, n_r\}$ which is a finite set of $m + r$ elements.
23. (a) Write $[a, b] = aba^{-1}b^{-1}$. Then $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$. Thus $x \mapsto gxg^{-1}$ permutes the generators $[a, b]$; so, preserves the subgroup generated by $[a, b]$ for all $a, b \in G$. Thus the commutator subgroup is normal.
- (b) For two elements $aG', bG' \in G/G'$, we find

$$G'aG'b = G'ab = G'aba^{-1}b^{-1}ba = G'[a, b]ba = G'ba = G'bG'a;$$

so, G/G' is commutative.

7.8

2. Easy! because $f(e, b) = b$ for any given $b \in H$.
3. (a) $(x, y)(a, e_H)(x, y)^{-1} = (xax^{-1}, ye_Hy^{-1}) = (xax^{-1}, e_H) \in G^*$; so,
- $$(x, y)G^*(x, y)^{-1} \subset G^*.$$

Then by Theorem 7.34 (3), G^* is normal.

- (b) Verify that the function $f(a) = (a, e_H)$ gives an isomorphism $G \cong G^*$.
- (c) Define $p : (G \times H)/G^* \rightarrow H$ by $p((x, y)G^*) = y$, and show that this is an isomorphism.

5. Hint: First prove that (i) every subgroup of a cyclic group C_n of order n is cyclic and has order a factor of n , and (ii) for a given factor d of n and the generator c , such subgroup is generated by $c^{n/d}$ and hence unique.
6. Hint: First prove that for a given subgroup H of a cyclic group C_n of order n , C_n/H is cyclic of order $n/|H|$.
13. Define $f : G \rightarrow G/N$ by $f(x) = xN$. Then verify that f is a homomorphism. Check that $K = f^{-1}(K')$ for $K' = K/N$. Then for $x \in G$ and $k \in K$, $f(xkx^{-1}) = f(x)f(k)f(x)^{-1} \in K'$ because of normality of K' . Thus $xkx^{-1} \in f^{-1}(K') = K$; so, $xKx^{-1} \subset K$; so, K is normal.
18. (a) Define N by $f^{-1}(M) = \{g \in G | f(g) \in M\}$. Verify that N is a subgroup and satisfies the required property.
- (b) Proceed as in Exercise 13.

7.9

8. Just rotate i -times a_1, a_2, \dots, a_6 . For example $\sigma^2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \end{pmatrix}$.
13. Since disjoint cycles x_1, \dots, x_m commutes each other, we have

$$(x_1x_2 \cdots x_m)^n = x_1^n x_2^n \cdots x_m^n.$$

If n is the LCM of $|x_j|$, we have $n = |x_j|n_j$ and hence $x_j^n = (x_j^{|x_j|})^{n_j} = e$. Thus $(x_1x_2 \cdots x_m)^n = e$ and hence $k = |x_1x_2 \cdots x_m| \mid n$ (Theorem 7.8). On the other hand, since x_j are disjoint, $(x_1x_2 \cdots x_m)^k = e$ implies $x_j^k = e$. Thus in particular $|x_j| \mid k$ for all j . So k is the multiple of the LCM n . This implies $k = n$.

16. As we have seen in the solution of Exercise 11 in Section 7.7, $\sigma(ab)\sigma^{-1} = (\sigma(a)\sigma(b))$. Thus if $\sigma \in Z(S_n)$, $(\sigma(a), \sigma(b)) = (ab)$ for all two distinct integer $1 \leq a < b \leq n$. This is only possible when $\sigma(a) = a$ for all a ; so, σ has to be the identity.

8.1

6. (a) $\mathbb{Z}_{12} = \langle 3 \rangle \times \langle 4 \rangle$.
 (b) $\mathbb{Z}_{15} = \langle 3 \rangle \times \langle 5 \rangle$.
 (c) $\mathbb{Z}_{30} = \langle 15 \rangle \times \langle 10 \rangle \times \langle 6 \rangle$.
7. The operation is component-wise; so, commutativity follows from component-wise commutativity and vice-versa.
4. $|a^3| = 5$; thus $|H| = 5$. This shows $[G : H] = \frac{15}{5} = 3$; so, there are three cosets: $H, Ha = \{a, a^4, a^7, a^{10}, a^{13}\}, Ha^2 = \{a^2, a^5, a^8, a^{11}, a^{14}\}$.
8. Same as Exercise 2 of Section 7.8.
16. Identify G with $N \times K$ by an isomorphism $f : G \cong N \times K$ given by $f(nk) = (n, k)$. Then N corresponds to $N \times \{e_K\}$; in other words, $f(N) = N \times \{e_K\}$. Then $(x, y)(m, e_K)(x, y)^{-1} = (xmx^{-1}, ye_Ky^{-1}) = (xmx^{-1}, e_K)$. Since M is normal in N , $xmx^{-1} \in M$; so, $f(M)$ is normal in $N \times K$. Thus N is normal in G .

8.2

10. Check by yourself that f is a homomorphism. We are going to show that f is a bijection. First suppose that G is finite. Let $|G| = p^m$. Then $p^m x = 0$ for every $x \in G$. Take integers k and j so that $1 = nk + jp^m$ (Linear equation theorem: Theorem 1.3). Then $x = nkx + jp^m x = nkx$ for $x \in G$; so, f is surjective. Since G is finite, f has to be injective also. Thus f is an isomorphism. When G is infinite, $\langle x \rangle$ is a finite p -group for each $x \in G$. Thus $f : \langle x \rangle \rightarrow \langle x \rangle$ is an isomorphism. In particular $f : G \rightarrow G$ is surjective. Take $x, y \in G$ with $f(x) = f(y)$. Then $\langle x, y \rangle$ is a finite p -group. So $f : \langle x, y \rangle \rightarrow \langle x, y \rangle$ is an isomorphism; in particular, it is injective on $\langle x, y \rangle$ and hence $x = y$. This shows that f is injective on the entire G . Thus f is an isomorphism.
11. Define $[m]x = mx$ for the class of m in \mathbb{Z}_p . If $m \equiv n \pmod{p}$, then $n = m + kp$ for an integer k ; so, $(m + kp)x = mx + kpx = mx + 0 = mx$; thus, $[m]x$ is well defined independently of the choice of the representative m . Verify that by this multiplication, G is a vector space over a field \mathbb{Z}_p . Then choose a base x_1, \dots, x_n of G over \mathbb{Z}_p . The dimension n is finite because G is a finite group. Then every element $x \in G$ is a unique linear combination $x = a_1x_1 + \cdots + a_nx_n$ for $a_j \in \mathbb{Z}_p$. Then define $f : G \rightarrow \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ by $f(x) = (a_1, \dots, a_n)$. Then prove yourself that f is an isomorphism.

12. By Theorem 8.5, $G(p)$ contains non-identity x . Then $|x| = p^m$. Then $p^{m-1}x$ has order p (see the solution of Exercise 14 of Section 7.2).
14. By Theorem 8.5, $G = G(p) \times G(q_1) \times \cdots \times G(q_r)$ for prime factors q_j of m which are different from p . By Exercise 13, $G(q_i)$ has order $q_i^{j_i}$ and $G(p)$ has order p^j . Since $p^t m = |G| = p^j q_1^{j_1} \cdots q_r^{j_r}$, we find that $p^t = p^j$, because q_j divides m and m does not have factor p .
15. By Exercise 14, if $|G|$ is exactly divisible by p^t , then $G(p)$ has order p^t ; so, we need to find a subgroup $H \subset G(p)$ with given order p^s with $s < t$. By Fundamental theorem of finite abelian groups, $G(p) \cong \mathbb{Z}_{p^{m_1}} \oplus \mathbb{Z}_{p^{m_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_r}}$. Since $t = m_1 + m_2 + \cdots + m_r$, we can find integers n_j with $0 < n_j \leq m_j$ such that $s = n_1 + n_2 + \cdots + n_r$. Then each $\mathbb{Z}_{p^{m_j}}$ has the unique finite subgroup $\langle p^{m_j - n_j} \rangle$ of order p^{n_j} . Then $H = \langle p^{m_1 - n_1} \rangle \oplus \cdots \oplus \langle p^{m_r - n_r} \rangle$ in $G(p)$ has the desired order p^s .
16. If n contains a prime power p^m with $m \geq 2$, we have at least two non-isomorphic abelian group of order n : these are the cyclic group: \mathbb{Z}_n and $\mathbb{Z}_p \oplus \mathbb{Z}_{p^{m-1}} \oplus \mathbb{Z}_{n/p^m}$. Thus n has to be square-free (that is, no square prime factor). If n is square-free, any abelian group of order n is a cyclic group of order n , because its elementary divisor is just a single n .