Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 10
December 5, 2007

Section 7.7

4. First notice that $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ is abelian, so N and every other subgroup is normal. This implies that G/N has the structure of a group. We can determine this structure most directly by constructing the group table for the quotient group. First, the elements in N are $N = \{(0,0),(3,2),(2,0),(1,2)\}$. The distinct cosets are

$$(0,0)+N, (0,1)+N = \{(0,1),(3,3),(2,1),(1,3),$$
$$(0,2)+N = \{(1,0),(0,2),(3,0),(2,2)\}\}, (0,3)+N = \{(1,1),(0,3),(3,1),(2,3)\}.$$

Then the group table for the quotient group G/N is constructed using the coset addition operation (omitting $+N$'s for simplicity):

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$
$(0,2)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$
$(0,3)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$

For example, $(0,2)+N+(0,3)+N = (0,1)+N$ from the above. By inspection, G/N is isomorphic to the cyclic group of order 4, $\mathbb{Z}_4$, since the coset $(0,1)+N$ is a generator for the whole group.

5. We proceed as in 4 above. $N = \{(0,0),(1,1),(2,0),(3,1),(4,0),(5,1)\}$ Hence $(1,1)$ is an element of order 6, and by Lagrange's Theorem $|G/N| = 2$. There are two cosets of N in G, $N = (0,0)+N$ and $(0,1)+N = \{(0,1),(1,0),(2,1),(3,0),(4,1),(5,0)\}$. The quotient group is isomorphic to $\mathbb{Z}_2$ (every group of order 2 is isomorphic to $\mathbb{Z}_2$ since 2 is prime).

6. This could also be done by constructing the group tables of U_{32}/N and U_{16} and comparing their structures. We will illustrate a different method in this solution. We have that $U_{32} = \{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}$ is an abelian group of order 16 under *multiplication* mod 32. The subgroup $N = \{1,17\}$ has 8 distinct multiplicative cosets, one for each $k = 1,3,5,7,9,11,13,15$. This true because if $k = 2\ell+1$, then $17k = (16+1)(2\ell+1) = 32\ell+16+(2\ell+1) \equiv 16+k \bmod 32$. For instance, this says $N\cdot 5 = \{5,21\}$, etc. We construct

$$\begin{aligned} \varphi : U_{32}/N &\to U_{16} \\ N\cdot k &\mapsto [k]_{16} \end{aligned}$$

This is well defined since if $N\cdot k = N\cdot \ell$, then by the above $k \equiv \ell \bmod 16$, so they define the same class in U_{16}. The mapping φ is one-to-one and onto by construction. It is a group homomorphism because

$$\varphi((N\cdot k)(N\cdot \ell)) = \varphi(N\cdot(k\ell)) = [k\ell]_{16} = [k]_{16}[\ell]_{16} = \varphi(N\cdot k)\varphi(N\cdot \ell).$$

Therefore U_{32}/N and U_{16} are isomorphic groups.

8. Let $Nx \in G/N$. Then by the definition of the coset product operation and the fact that $x^2 \in N$, $(Nx)^2 = (Nx)(Nx) = Nx^2 = N = Ne$. Since Ne is the identity element in G/N. This shows that if $Nx \neq Ne$, then Nx has order 2 in G/N.

9. N is automatically normal in G, so G/N is a group. Let Na and Nb be any two cosets. Then by the definition of the coset product and the fact that G is abelian,

$$(Na)(Nb) = N(ab) = N(ba) = (Nb)(Na).$$

This shows that G/N is an abelian group.

15. (a) Let $p/q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. The operation is addition, so

$$q \cdot (p/q + \mathbb{Z}) = (p/q + p/q + \cdots + p/q) + \mathbb{Z} = p + \mathbb{Z} = \mathbb{Z} = 0 + \mathbb{Z}.$$

This shows that $p/q + \mathbb{Z}$ has finite order (equal to some divisor of the integer q).

(b) Let p/q be a rational number in lowest terms (that is, $(p, q) = 1$). Then when we form $q(p/q + \mathbb{Z}) = 0 + \mathbb{Z}$, no smaller multiple of $p/q + \mathbb{Z}$ equals $0 + \mathbb{Z}$ since the smallest positive multiple of p that is also a multiple of q is pq. This shows that $\mathbb{Q}/\mathbb{Z}$ contains elements of every order $q \geq 1$.

16. The result in part (a) of Exercise 15 also shows that every element of the subgroup $\mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$ has finite order in $\mathbb{R}/\mathbb{Z}$. Now let $r \in \mathbb{R}/\mathbb{Z}$ and assume that there is some positive integer q such that $0 + \mathbb{Z} = q(r + \mathbb{Z}) = qr + \mathbb{Z}$. This is only true if $qr = p \in \mathbb{Z}$. But then $r = p/q \in \mathbb{Q}$. Hence the set of elements of finite order in $\mathbb{R}/\mathbb{Z}$ is contained in $\mathbb{Q}/\mathbb{Z}$. Since both containments hold, the two subgroups are equal.

23. (a) Let $a, b \in G$, then following the hint, for all $g \in G$,

$$g^{-1}aba^{-1}b^{-1}g = (g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) = (g^{-1}ag)(g^{-1}bg)(g^{-1}ag)^{-1}(g^{-1}bg)^{-1} \in G'.$$

If we have any element c of G', then $c = c_1c_2 \cdots c_n$ is a product of elements $c_i = a_ib_ia_i^{-1}b_i^{-1}$ of the form above for $i = 1, \ldots, n$. Hence $g^{-1}cg = (g^{-1}c_1g)(g^{-1}c_2g) \cdots (g^{-1}c_ng)$ is also a product of commutators, hence an element of G'. This shows $g^{-1}G'g \subseteq G'$ for all $g \in G$. Hence G' is normal by part (2) of Theorem 7.34.

(b) In the quotient group G/G', consider any two cosets $G'a$ and $G'b$. By the definition of the coset product, we have

$$(G'a)(G'b)(G'a)^{-1}(G'b)^{-1} = G'(aba^{-1}b^{-1}) = G' = G'e,$$

since $aba^{-1}b^{-1} \in G'$. This implies $(G'a)(G'b) = (G'b)(G'a)$ for all a, b. Hence G/G' is an abelian group.

Section 7.8

6. (a) Every subgroup of $\mathbb{Z}_{12}/H$ is K/H for a subgroup $K \subset \mathbb{Z}_{12}$ containing H (Theorem 7.44, part (3)). These subgroups are $K_0 = H$ itself, $K_1 = \{0, 3, 6, 9\}$, $K_2 = \{0, 2, 4, 6, 8, 10\}$, and $K_3 = \mathbb{Z}_{12}$. The corresponding subgroups of $\mathbb{Z}_{12}/H$ are $K_0/H = \{0 + H\}$, $K_1/H = \{0 + H, 3 + H\}$, $K_2/H = \{0 + H, 2 + H, 4 + H\}$, and $K_3/H = \mathbb{Z}_{12}/H = \{0 + H, 1 + H, 2 + H, 3 + H, 4 + H, 5 + H\}$.

(b) Similar to part (a). This time there are only three such subgroups, L_i/K where $L_0 = K$, $L_1 = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$, and $L_2 = \mathbb{Z}_{20}$.

10. (a) The set K is the set of all elements of order 2 or less. Since $e \in G$ has order 1, K is nonempty. Moreover, if $a, b \in K$, then using the abelian hypothesis on G, $(ab)^2 = (ab)(ab) = a^2b^2 = e$. Hence ab has order at most 2 and is an element in K. Finally, if $a \in G$, then the order of a^{-1} is the same as the order of a, so $a^{-1} \in K$ as well. Thus K is a subgroup of G.

(b) The set H is the set of squares of elements in G. This is nonempty since G is nonempty. If $a = x^2$ and $b = y^2$ are in H, then $ab = x^2y^2 = (xy)(xy) = (xy)^2$ is also in H since x and y commute. Finally, if $a = x^2$ is in H, then $a^{-1} = (x^2)^{-1} = (x^{-1})^2 \in H$. Hence H is a subgroup of G.

(c) Let $\varphi : G \to H$ be the mapping $\varphi(x) = x^2$. This is a group homomorphism under the hypothesis that G is abelian: $\varphi(xy) = (xy)^2 = (xy)(xy) = x^2y^2 = \varphi(x)\varphi(y)$. By definition φ is onto H. The kernel of φ is precisely the subgroup K from part (a). Hence by the First Isomorphism Theorem, $H \simeq G/K$.

15. The group $\mathbb{R}^*$ is the multiplicative group of nonzero reals. The mapping

$$\begin{aligned} \det : \mathrm{GL}(2, \mathbb{R}) &\to \mathbb{R}^* \\ A &\mapsto \det(A) \end{aligned}$$

is a group homomorphism by Exercise 22 of section 7.6. The kernel of det is the subgroup $\mathrm{SL}(2, \mathbb{R})$ (this was one way to show that $\mathrm{SL}(2, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(2, \mathbb{R})$ – see Exercise 23 of section 7.6). Hence by the First Isomorphism Theorem, $\mathrm{GL}(2, \mathbb{R})/\mathrm{SL}(2, \mathbb{R}) \simeq \mathbb{R}^*$.

16. (a) By the distributive law in R, $f(x+y) = r(x+y) = rx+ry = f(x)+f(y)$. Hence $f : R \to R$ is a group homomorphism for the additive group structure on $(R, +)$.

(b) Let $R = \mathbb{Z}$ and $r = 4 \in \mathbb{Z}$. Then $f(1 \cdot 2) = 4 \cdot (1 \cdot 2) = 8$ but $f(1) \cdot f(2) = (4 \cdot 1) \cdot (4 \cdot 2) = 32$. Hence $f(1 \cdot 2) \neq f(1) \cdot f(2)$. So f is not a ring homomorphism from $\mathbb{Z}$ to itself.

(c) Suppose that R is a commutative ring and r is an *idempotent* element (that is $r^2 = r$). Then $f(xy) = r(xy) = r^2(xy) = (rx)(ry) = f(x)f(y)$. So in this case f is a ring homomorphism. (*Comment:* Another correct answer would be to say that $r = 0, 1$ always work! Any ring R contains idempotents $r = 0, 1$. Some rings have others too. For instance, $R = \mathbb{Z} \times \mathbb{Z}$ under the component-wise sum and product operations also has idempotents $r = (1, 0)$ and $r = (0, 1)$.)

17. (a) G is clearly nonempty since $a, b, c \in \mathbb{Q}$ are arbitrary. Let

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1 & a+a' & b+ac'+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}. \tag{1}$$

Since this matrix is also in G, G is closed under matrix multiplication. The computation above also shows that $AB = I$, the 3×3 identity matrix, if $a' = -a, c' = -c$, and $b' = -b - ac' = -b + ac$. The matrix

$$B = A^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

is also in G. Hence G is a subgroup of $\mathrm{GL}(3, \mathbb{Q})$, hence a group.

(b) From the equation for AB above and the reverse product

$$BA = \begin{pmatrix} 1 & a'+a & b'+a'c+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix},$$

we see that $AB = BA$ if and only if $a'c = ac'$. Hence A is in the center of G if and only if $a'c = ac'$ *for all choices of* $a', c' \in \mathbb{Q}$. For $a' = 1, c' = 0$ we get $c = 0$ and then since $c' \neq 0$ is also possible, $a = 0$ as well. The center of G is

$$Z(G) = \left\{ A \in G : A = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b \in \mathbb{Q} \right\}.$$

To show the last statement in this part, consider the mapping

$$\varphi : Z(G) \to \mathbb{Q}$$

defined by

$$\varphi\left(\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) = b.$$

This is clearly one-to-one and onto, and moreover by the product formula (1) above in the case $a = c = a' = c' = 0$, we see if A and B are as in part A, $\varphi(AB) = b + b' = \varphi(A) + \varphi(B)$. This shows that $Z(G)$ and $(\mathbb{Q}, +)$ are isomorphic groups.

(c) Now define $\psi : G \to \mathbb{Q} \times \mathbb{Q}$ (a group under component-wise sums) by

$$\psi\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, c).$$

By the product formula (1), ψ is a group homomorphism: $\psi(AB) = (a+a', c+c') = (a, c)+(a', c') = \psi(A) + \psi(B)$. Then we note that $\ker(\psi)$ is the set of matrices A in G with $a = c = 0$. This is precisely $Z(G)$ by part (b). Hence by the First Isomorphism Theorem, $\mathbb{Q} \times \mathbb{Q} \simeq G/Z(G)$.

Section 7.9

3. (a) This is (12)(45)(679). (b) (13)(254)(789). (c) (13)(254)(69)(78). (d) (1573)(24). (e) (123)(456)(78).

4. (a) One way (there are many other correct ones too – see for instance the different factorization from Corollary 7.48!): (12)(45)(79)(69). (b) (13)(54)(24)(89)(69). (c) (13)(54)(24)(69)(78). (d) (73)(53)(13)(24). (e) (23)(13)(56)(46)(78).

5. (a) $(2468) = (68)(48)(28)$ is odd. (b) even. (c) even.

23. Let $\tau = (ij)$. Then we claim that for any $\sigma \in S_n$, $\rho = \sigma\tau\sigma^{-1} = (\sigma(i)\sigma(j))$. To see this note that $\rho(\sigma(i)) = \sigma(\tau(i)) = \sigma(j)$ and $\rho(\sigma(j)) = \sigma(\tau(j)) = \sigma(i)$. Moreover if k is any element of $\{1, 2, \ldots, n\}$ besides $\sigma(i), \sigma(j)$ then we can write $k = \sigma(\ell)$ for some $\ell \neq i, j$. Then $\rho(k) = \sigma(\tau(\ell)) = \sigma(\ell) = k$. Hence ρ fixes every other element of $\{1, 2, \ldots, n\}$ besides i, j. Therefore $\rho = \sigma\tau\sigma^{-1} = (\sigma(i)\sigma(j))$ is a transposition.

24. We combine Exercise 23 and the factorization of the cycle τ as a product of transpositions as in Corollary 7.48. We have $(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$. Hence

$$\begin{aligned} \sigma(a_1 a_2 \cdots a_k)\sigma^{-1} &= \sigma(a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)\sigma^{-1} \\ &= (\sigma(a_1 a_k)\sigma^{-1})(\sigma(a_1 a_{k-1})\sigma^{-1}) \cdots (\sigma(a_1 a_2)\sigma^{-1}) \\ &= (\sigma(a_1)\sigma(a_k))(\sigma(a_1)\sigma(a_{k-1})) \cdots)(\sigma(a_1)\sigma(a_2)) \\ &= (\sigma(a_1)\sigma(a_2) \cdots \sigma(a_k)) \end{aligned}$$

25. Consider $H = G \cap A_n$, which is a subgroup of G. H consists of all the even permutations that are in H. But now since there is some $\sigma \in G$ that is an odd permutation, we can consider the right coset $H\sigma$. Every element of the coset $H\sigma$ is an odd permutation that is in G. Moreover every odd ρ permutation in G has the form $\rho = (\rho\sigma^{-1})\sigma$. Since ρ and σ are odd, $\rho\sigma^{-1}$ is even, so it is an element of H. Therefore every odd permutation in G belongs to the coset $H\sigma$. Hence $H \cap H\sigma = G$, since every permutation in G is either even or odd. This shows that H has index 2 in G.

Section 8.1

5. The Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4, but no elements of order 4 (only orders 1 and 2). Therefore $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic even though $\mathbb{Z}_2 = \langle 1 \rangle$ is a cyclic group.

6. (a) Every element of $\mathbb{Z}_{12}$ can be written uniquely as a sum of an element of $H = \{0, 3, 6, 9\}$ and $K = \{0, 4, 8\}$. (the cosets of H for the elements in K fill out all of $\mathbb{Z}_{12}$). Hence by Theorem 8.1, $\mathbb{Z}_{12} \simeq H \times K$.

(b) Every element of $\mathbb{Z}_{15}$ can be written uniquely as a sum of an element of $H = \{0, 5, 10\}$ and $K = \{0, 3, 6, 9, 12\}$ (the cosets of H for the elements in K fill out all of $\mathbb{Z}_{15}$). Hence by Theorem 8.1, $\mathbb{Z}_{15} \simeq H \times K$. 7.

(c) Finally, every element of $\mathbb{Z}_{30}$ can be written uniquely as a sum of an element of $H = \{0, 5, 10, 15, 20, 25\}$ and $K = \{0, 6, 12, 18, 24\}$. Hence by Theorem 8.1, $\mathbb{Z}_{30} \simeq H \times K$. Similarly, $\mathbb{Z}_{30} \simeq \{0, 10, 20\} \times \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$. and

$$\mathbb{Z}_{30} \simeq \{0, 15\} \times \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}.$$

Note that we also have

$$\mathbb{Z}_{30} = \{0, 15\} \times \{0, 10, 20\} \times \{0, 6, 12, 18, 24\}.$$

7. $\Rightarrow$: If $G_1 \times G_2 \times \cdots \times G_n$ is an abelian group, then for each i, $1 \leq i \leq n$, and all $a, b \in G_i$,

$$(e_1, \ldots, e_{i-1}, a, e_{i+1}, \ldots, e_n)(e_1, \ldots, e_{i-1}, b, e_{i+1}, \ldots, e_n) = (e_1, \ldots, e_{i-1}, ab, e_{i+1}, \ldots, e_n)$$

and

$$(e_1, \ldots, e_{i-1}, b, e_{i+1}, \ldots, e_n)(e_1, \ldots, e_{i-1}, a, e_{i+1}, \ldots, e_n) = (e_1, \ldots, e_{i-1}, ba, e_{i+1}, \ldots, e_n).$$

The left sides of these equations are equal, hence the right sides are equal too, so $ab = ba$. This shows G_i is abelian.

$\Leftarrow$: Suppose each G_i is abelian. Then in the direct product for all $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$,

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) = (b_1 a_1, \ldots, b_n a_n) = (b_1, \ldots, b_n)(a_1, \ldots, a_n)$$

This shows that the direct product is also an abelian group.

9. The answer is *No*. One reason we can see this is that $\mathbb{Z}_4 \times \mathbb{Z}_2$ contains only elements of order $1, 2, 4$ (none of order 8):

$$\begin{aligned} 1 &= |(0,0)| \\ 2 &= |(2,0)| = |(2,1)| = |(0,1)| \\ 4 &= |(1,0)| = |(1,1)| = |(3,0)| = |(3,1)|. \end{aligned}$$

This shows that $\mathbb{Z}_4 \times \mathbb{Z}_2$ cannot be isomorphic to the cyclic group $\mathbb{Z}_8$.