Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 8
November 1, 2007

Section 7.1

9.

(a) The order of U_n is the number of k, $0 \leq k \leq n-1$ that are relatively prime to n. So $U_{10} = \{1,3,7,9\}$ has order 4, $U_{12} = \{1,5,7,11\}$ has order 4 and $U_{24} = \{1,5,7,11,13,17,19,23\}$ has order 8. *Comment:* The numbers of elements here are values of a famous function called "Euler's ϕ-function." It can be shown that the number of k as above relatively prime to n is given by the following formula if the prime factorization of $n = p_1^{e_1} \cdots p_s^{e_s}$:

$$\phi(n) = p_1^{e_1-1}(p_1-1)\cdots p_s^{e_s-1}(p_s-1).$$

For instance $24 = 2^3 \cdot 3$, so $\phi(24) = 2^2(2-1)\cdot 3^0(3-1) = 8$.

(b) $U_{20} = \{1,3,7,9,11,13,17,19\}$ (order 8). The orders of the elements are

$$\begin{aligned} |1| &= 1 \text{ (it's the identity element)} \\ |9| = |11| = |19| &= 2 \text{ since for instance } 9^2 = 81 \equiv 1 \bmod 20 \\ |3| = |7| = |13| = |17| &= 4 \text{ since } 3^2 \equiv 7^2 \equiv 13^2 \equiv 17^2 \equiv 9 \bmod 20 \end{aligned}$$

10.

a. In $\mathbb{Z}_4$, $|0| = 1, |1| = 4, |2| = 2, |3| = 4$.

b. In $\mathbb{Z}_4 \times \mathbb{Z}_2$, $|(0,0)| = 1$, $|(1,0)| = |(1,1)| = |(3,0)| = |(3,1)| = 4$, and $|(0,1)| = |(2,0)| = |(2,1)| = 2$.

c. In S_3, $|()| = 1$, $|(123)| = |(132)| = 3$, and $|(12)| = |(13)| = |(23)| = 2$.

d. (Using Hungerford's notation), $|r_0| = 1$, $|r_1| = |r_3| = 4$, and $|r_2| = |d|, |t|, |h|, |v| = 2$.

e. In $\mathbb{Z}$, 0 has order 1, but every other element has infinite order.

16. We have $x = a_1 a_2 \cdots a_n$, so $x^2 = (a_1 a_2 \cdots a_n)(a_1 a_2 \cdots a_n)$. G is a group, so each of the a_i has an inverse in G. This inverse must be one of the factors appearing in the second product. Since G is abelian, we can rearrange the factors to write $x^2 = (a_1 a_1^{-1})(a_2 a_2^{-1}) \cdots (a_n a_n^{-1}) = e$, which is what we wanted to show.

22. If $(ab)^2 = a^2 b^2$, then we have $abab = aabb$ in G. Since G is a group each element has an inverse in G, so we can multiply the given equation on both sides by a^{-1} on the left and b^{-1} on the right:

$a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}$. After simplifying, we get $ba = ab$. Since this is true for all $a, b \in G$, G is abelian.

25. We assume that every $a \neq e$ in G has order 2, so $a^2 = a$, and hence $a = a^{-1}$. It follows that *every element of* G satisfies $a = a^{-1}$, since this is true of e as well. If a, b are any two elements of G, then by the "reverse order" rule for the inverse of a product: $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. Hence G is abelian.

30. Consider the mapping $\iota : G \to G$ where $\iota(g) = g^{-1}$. Then $\iota(e) = e$, and if $g \in G$, then $\iota(\iota(g)) = (g^{-1})^{-1} = g$. If g is an element of order > 2 then g and $\iota(g)$ are distinct, and are interchanged by ι. Hence, "pairing up" elements with their inverses via ι, since $|G|$ is even, there must be at least one other element $g \in G$ other than e with $\iota(g) = g$. Since $g^{-1} = g$, $g^2 = e$ but $g \neq e$. This shows that G must contain an element of order 2.

Section 7.3

6. The definition of H is equivalent to saying that $H = \{a \in G : a^k = e\}$ for the fixed integer k. We use Theorem 7.10 to show that H is a subgroup of G when G is abelian. Notice that H is nonempty since $e^k = e$ implies $e \in H$. Next, if $a, b \in H$, then $a^k = b^k = e$. Consider $ab \in G$. Since G is assumed abelian we can reorder the factors to rewrite $(ab)^k = (ab)(ab)\cdots(ab) = (aa\cdots a)(bb\cdots b) = a^k b^k$. Since $a, b \in H$, this shows $(ab)^k = e$, so $ab \in H$. Finally, let $a \in H$, so $a^k = e$. This implies $e = (a^k)^{-1} = (a^{-1})^k$. Hence $a^{-1} \in H$ as well. It follows that H is a subgroup of G.

7. We reason as in problem 6 above, but now note that if $a \in T$, then the power $k > 0$ such that $a^k = e$ will vary with which element a we are considering. Notice that T is nonempty since $e^k = e$ implies $e \in H$. Next, if $a, b \in T$, then $a^k = b^\ell = e$ for some integers k, ℓ. Consider $ab \in G$, and let $m = k\ell$. Since G is assumed abelian we can reorder the factors to rewrite $(ab)^m = (ab)(ab)\cdots(ab) = (aa\cdots a)(bb\cdots b) = a^m b^m$. Then $a^m = (a^k)^\ell = e$ and $b^m = (b^\ell)^k = e$. This shows $(ab)^m = e$, so $ab \in T$. Finally, let $a \in T$, so $a^k = e$ for some $k > 0$. This implies $e = (a^k)^{-1} = (a^{-1})^k$. Hence $a^{-1} \in T$ as well. It follows that T is a subgroup of G.

15. This is *false*. The group S_3 gives a counterexample since every proper subgroup of S_3 is cyclic of order 2 or 3, but S_3 is not cyclic itself. There are no elements of order 6 in S_3.

16. We must show that $\mathbb{Q}^{**}$ is not equal to $\langle r \rangle$ for any $r \in \mathbb{Q}^{**}$. Certainly $r = 1$ does not work since $\{1^k : k \in \mathbb{Z}\} = \{1\}$ is the trivial subgroup. So consider $r \neq 1$ and the subgroup $\langle r \rangle$. Without loss of generality, we may assume $r > 1$, since if $r < 1$, then $r^{-1} = \frac{1}{r} > 1$, and $\langle r \rangle = \langle r^{-1} \rangle$. If $r > 1$, then the elements of $\langle r \rangle$ are ordered as follows in $\mathbb{R}$:

$$0 < \cdots r^{-2} < r^{-1} < 1 < r < r^2 < r^3 < \cdots$$

Recall from Principles of Analysis (MATH 242) that the set of rational numbers is *dense* in $\mathbb{R}$. In other words, in every interval of positive length in $\mathbb{R}$, there are rational numbers. In particular, there must be rational numbers s in the open interval $(1, r)$. Any such rational number s is in $\mathbb{Q}^{**}$,

since $s > 0$. But $s \neq r^k$ for any k because of the way the powers of r are ordered as above. This shows that $\langle r \rangle$ is not all of $\mathbb{Q}^{**}$. Since this is true for all $r \neq 1$, $\mathbb{Q}^{**}$ is not a cyclic group.

20. First note that if $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, then $(a, b) = a(1, 0) + b(0, 1)$. So the set $\{(1, 0), (0, 1)\}$ generates $\mathbb{Z} \times \mathbb{Z}$. On the other hand,

$$(1, 0) = (3, 1) + (-2, -1) \text{ and } (0, 1) = 2(-2, -1) + (4, 3).$$

Hence for any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, we have

$$\begin{aligned} (a, b) &= a(1, 0) + b(0, 1) \\ &= a((3, 1) + (-2, -1)) + b(2(-2, -1) + (4, 3)) \\ &= a(3, 1) + (a + 2b)(-2, -1) + b(4, 3). \end{aligned}$$

This shows $\mathbb{Z} \times \mathbb{Z}$ is contained in the subgroup generated by $\{(3, 1), (-2, -1), (4, 3)\}$. The opposite inclusion is true by definition. Hence $\{(3, 1), (-2, -1), (4, 3)\}$ generates $\mathbb{Z} \times \mathbb{Z}$.

21. (a) Check that the element $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6:

$$(0, 0), (1, 1), 2 \cdot (1, 1) = (0, 2), 3 \cdot (1, 1) = (1, 0), 4 \cdot (1, 1) = (0, 1), 5 \cdot (1, 1) = (1, 2).$$

Since we have all 6 elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$, this group is the same as the cyclic subgroup $\langle (1, 1) \rangle$, hence cyclic.
(b) The cyclic subgroups are

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

Since none of these is of order 8, $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic. However, $\mathbb{Z}_2 \times \mathbb{Z}_4$ is generated by $(1, 0)$ and $(0, 1)$.

30. (a) We use Theorem 7.10 to show that HK is a subgroup when G is abelian. First, $HK \neq \emptyset$ since $e \in H$ and $e \in K$, so $e \cdot e = e \in HK$. If $a, b \in HK$, then $a = h_1 k_1$ and $b = h_2 k_2$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Since G is abelian,

$$ab = (h_1 k_1)(h_2 k_2) = h_1(k_1 h_2)k_2 = h_1(h_2 k_1)k_2 = (h_1 h_2)(k_1 k_2).$$

Since H and K are subgroups, $h_1 h_2 \in H$ and $k_1 k_2 \in K$. Therefore $ab \in HK$ and HK is closed under products. Finally if $a = hk \in HK$, then since G is abelian again,

$$a^{-1} = (hk)^{-1} = k^{-1} h^{-1} = h^{-1} k^{-1}.$$

Then $h^{-1} \in H$ and $k^{-1} \in K$ since H, K are subgroups of G. Therefore HK is also closed under inverses.

(b) Let $G = S_3$, and let $H = \{(), (12)\}$, $K = \{(), (13)\}$. Then

$$HK = \{()(), ()(13), (12)(), (12)(13)\} = \{(), (13), (12), (132)\}.$$

This is not a subgroup of S_3 since it is not closed under products or inverses. (*Comment:* Note, it even violates the necessary condition from the statement of Lagrange's Theorem!)

Section 7.4

3. (a) The group of invertible 2×2 matrices with entries in $\mathbb{Z}_2$ is $GL(2, \mathbb{Z}_2) =$

$$\left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, R^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

(These are all the 2×2 matrices of determinant 1 with $\mathbb{Z}_2$-entries, a group under matrix multiplication).

(b) Under the mapping $I \mapsto ()$, $R \mapsto (123)$, $R^2 \mapsto (132)$, $S \mapsto (13)$, $T \mapsto (12)$, $U \mapsto (23)$, we see that the group tables will "match up":

$\cdot$	I	R	R^2	S	T	U
I	I	R	R^2	S	T	U
R	R	R^2	I	U	S	T
R^2	R^2	I	R	T	U	S
S	S	T	U	I	R	R^2
T	T	U	S	R^2	I	R
U	U	S	T	R	R^2	I

and

$\circ$	()	(123)	(132)	(13)	(12)	(23)
()	()	(123)	(132)	(13)	(12)	(23)
(123)	(123)	(132)	()	(23)	(13)	(12)
(132)	(132)	()	(123)	(12)	(23)	(13)
(13)	(13)	(12)	(23)	()	(123)	(132)
(12)	(12)	(23)	(13)	(132)	()	(123)
(23)	(23)	(13)	(12)	(123)	(132)	()

5. U_5 is the group $\{1, 2, 3, 4\}$ under multiplication mod 5, while U_{10} is the group $\{1, 3, 7, 9\}$ under multiplication mod 10. Note that U_5 is cyclic with generator 2, since $2^2 = 4$, and $2^3 = 8 \equiv 3 \bmod 5$. Similarly U_{10} is cyclic since $3^2 = 9$ and $3^3 = 27 \equiv 7 \bmod 10$. The mapping $\varphi : U_5 \to U_{10}$ defined by

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(2) &= 3 \\ \varphi(4) &= 9 \\ \varphi(3) &= 7 \end{aligned}$$

is an isomorphism since it is injective and surjective, and $\varphi(2^k) = 3^k$ for all k, so

$$\varphi(2^k \cdot 2^\ell) = \varphi(2^{k+\ell}) = 3^{k+\ell} = 3^k \cdot 3^\ell = \varphi(2^k) \cdot \varphi(2^\ell).$$

10. Let $f : G \to H$ be a surjective homomorphism and assume G is abelian. Then for all $a, b \in H$, $a = f(x)$ and $b = f(y)$ for some $x, y \in G$ and therefore

$$ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba.$$

This establishes the desired fact that H is abelian, since the equation holds for all $a, b \in H$.

11. We will prove this for $n \geq 1$ by induction on n first. For the base case, we have $f(a^1) = f(a) = (f(a))^1$, so there is nothing to prove. Now assume that the statement is true for $n = k$. Since f is a group homomorphism, using the induction hypothesis at the second to last step:

$$f(a^{k+1}) = f(a^k \cdot a) = f(a^k) \cdot f(a) = (f(a))^k f(a) = (f(a))^{k+1}.$$

This establishes the statement for $n \geq 1$. The formula is clearly true for $n = 0$ since $f(a^0) = f(e) = e = (f(a))^0$. Finally, we show that the formula is true for $n = -m$ where $m \geq 1$ by another induction proof. For the base case here we need to see

$$f(a^{-1}) = (f(a))^{-1}.$$

This is true by part 2 of Theorem 7.19. Now assume the formula has been established for $m = k$. Then

$$f(a^{-(k+1)}) = f(a^{-k} \cdot a^{-1}) = f(a^{-k}) \cdot f(a^{-1}) = (f(a))^{-k}(f(a))^{-1} = (f(a))^{-(k+1)}.$$

This establishes the statement for $n \leq -1$ as well.

13. (a) We will ignore the hint and prove the parts separately. First we show that $a^{-1}Ha$ is a subgroup of G. First, $a^{-1}Ha$ is not empty since $a^{-1}ea = e \in a^{-1}Ha$. Next, let $x = a^{-1}ha$ and $y = a^{-1}ka$ be elements of $a^{-1}Ha$. Then

$$xy = (a^{-1}ha)(a^{-1}ka) = a^{-1}hka.$$

Since H is a subgroup, $hk \in H$. So $xy \in a^{-1}Ha$. This shows $a^{-1}Ha$ is closed under products. Last, if $x = a^{-1}ha \in a^{-1}Ha$, then $x^{-1} = (a^{-1}ha)^{-1} = a^{-1}h^{-1}(a^{-1})^{-1} = a^{-1}h^{-1}a \in a^{-1}Ha$, since $h^{-1} \in H$ (a subgroup). Hence $a^{-1}Ha$ is also a subgroup of G.

Now, we show that $a^{-1}Ha$ is isomorphic to H as a group. Consider the mapping $\varphi : G \to G$ defined by $\varphi(x) = a^{-1}xa$. (This is the "inner automorphism" mentioned in the problem.) We check that

$$\varphi(xy) = a^{-1}xya = a^{-1}x(aa^{-1})ya = (a^{-1}xa)(a^{-1}ya) = \varphi(x)\varphi(y).$$

This shows that φ is a group homomorphism. It is injective and surjective because φ has an inverse function $\psi(x) = axa^{-1}$: For all $x \in G$,

$$\varphi(\psi(x)) = a^{-1}(axa^{-1})a = x \text{ and } \psi(\varphi(x)) = a(a^{-1}xa)a^{-1} = x.$$

Then φ restricts to a mapping with domain H and range $a^{-1}Ha$, and similarly ψ restricts to a mapping with domain $a^{-1}Ha$ and range H. The restricted mappings are still inverses. This shows H and $a^{-1}Ha$ are isomorphic via φ.

(b) If H is finite then $a^{-1}Ha = \varphi(H)$ where φ is as in part a. Since φ is injective and surjective, $|H| = |a^{-1}Ha|$.

18. Let $G = \langle a \rangle$ and let $f : G \to H$ be a surjective group homomorphism. Then every element $b \in H$ is $b = f(c)$ for some $c \in H$. But by hypothesis, $c = a^n$ for some integer n. Hence using problem 11 above, $b = f(c) = f(a^n) = (f(a))^n$. This shows that every element of H is a power of $f(a)$, so $H \subset \langle f(a) \rangle$. The other inclusion is true by definition, hence $H = \langle f(a) \rangle$ is cyclic, generated by $f(a)$.