Mathematics 351 – Abstract Algebra 1
Solutions for Problem Set 9
November 9, 2007

Section 7.5 5. (a) $\mathbb{Z}_{24}$ has order 24, so by Lagrange's Theorem, the possible orders of subgroups of $\mathbb{Z}_{24}$ are $1, 2, 3, 4, 6, 8, 12, 24$.

(b) S_4 also has order $4! = 24$, so the possible orders of the subgroups of S_4 are the same as in part (a): $1, 2, 3, 4, 6, 8, 12, 24$.

(c) Since $|D_4| = 8$ and $|\mathbb{Z}_{10}| = 10$, we have $|D_4 \times \mathbb{Z}_{10}| = 80$. Hence the possible orders of subgroups of this group are all the divisors of 80: $1, 2, 4, 5, 8, 10, 16, 20, 40, 80$.

6. (a) Let $G = (\mathbb{Z} \times \mathbb{Z}, +)$, and let $H = \{(pa, b) : a, b \in \mathbb{Z}\}$. Then H is a subgroup of G. There only finitely many distinct cosets, namely the cosets

$$(0, 0) + H, (1, 0) + H, \ldots, (p - 1, 0) + H$$

(see the solution for problem 12 from Section 6.3 from Problem Set 7). Hence $[G : H] = p$ is finite.

(b) Let G be the same group as in part (a), but now let $H = \{(0, b) : b \in \mathbb{Z}\}$. The cosets $(a, 0) + H$ are all distinct. This follows since if $a \neq a'$, then $(a, 0) - (a', 0) = (a - a', 0) \notin H$, so $(a, 0) + H \neq (a', 0) + H$. Hence $[G : H]$ is infinite in this example.

7. The smallest possible order for such a group G is the least common multiple of the integers $1, 2, \ldots, 11, 12$. Thinking of the prime factorizations, 2, 3, $4 = 2^2$, 5, $6 = 2 \cdot 3$, 7, $8 = 2^3$, $9 = 3^2$, $10 = 5 \cdot 2$, 11, $12 = 2^2 \cdot 3$, we see that the least common multiple will be

$$N = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720.$$

8. The order n must satisfy $n < 100$ and $25|n$, $10|n$. This uniquely determines $n = 50 = \mathrm{lcm}(25, 10)$.

9. We are given that H and K are subgroups of G with $|H| = |K| = p$, p prime. Moreover $H \neq K$. We claim first that $H \cap K$ is a subgroup of H and of K. This follows since $H \cap K$ is not empty ($e \in H \cap K$). Then $a, b \in H \cap K$ implies $a, b \in H$ and $a, b \in K$. Hence $ab^{-1} \in H$ and $ab^{-1} \in K$ since H and K are subgroups. Thus, $ab^{-1} \in H \cap K$, so $H \cap K$ is a subgroup of G. Now by Lagrange's theorem, $|H \cap K|$ divides $|H| = p$ and $|K| = p$. But p is assumed prime, so $|H \cap K|$ is either 1 or p. If $|H \cap K| = p$, then $H \cap K = H = K$. Since we know that $H \neq K$, though, this means that $|H \cap K| = 1$. Hence $H \cap K = \{e\}$.

10. By the same fact we used in problem 9 above, $H \cap K$ is also a subgroup of G, hence of H and K as well. Then by Lagrange's theorem, we know that $|H \cap K|$ divides $|H|$ and $|K|$.

11. We will show first that G must be cyclic, and then deduce that the order of G must be prime. Since G has more than one element, let $a \in G$ be any element $a \neq e$. Then $\langle a \rangle$ is a subgroup of

G with more than one element. But by hypothesis, G has no non-proper subgroups. This implies that $\langle a\rangle = G$, so that G is a cyclic group. We claim next that G must be *finite*. This follows because if $G = \langle a\rangle$ was an infinite cyclic group, then G would contain proper subgroups like $\langle a^2\rangle$. This means that G is a finite cyclic group, so $G \simeq \mathbb{Z}_n$ for some $n > 1$ (Theorem 7.18). Now we claim that n must be prime. If not, then $n = km$ for some integers $k, m > 1$. But then the order of a^k is $m < n$. This implies that $|\langle a^k\rangle| = m$. But then $1 < m < n$ is the order of a subgroup of G, which contradicts the hypothesis that G has no non-proper subgroups.

13. The order is $30/\gcd(4, 30) = 15$. This can be seen directly by computing the powers of a^4 and using $a^{30} = e$:

$$e, a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}, a^{28}, a^{32} = a^2, a^6, a^{10}, a^{14}, a^{18}, a^{22}, a^{26}, a^{30} = e.$$

This shows that the order of a^4 is 15, so $|\langle a^4\rangle| = 15$ as well. Then the index of $\langle a^4\rangle$ in $\langle a\rangle$ is $|\langle a\rangle|/|\langle a^4\rangle| = 30/15 = 2$.

19. If $|G| = pq$ with p, q primes, then the possible orders of subgroups of G are the divisors of pq, namely $1, p, q, pq$. The proper subgroups of G have order p or order q. Since both of these are primes, all the proper subgroups of G must be cyclic by Theorem 7.28.

24. We will show this by considering two cases. If $|G| = 33$ and G has an element a of order 33 (that is, if G is cyclic), then G also has elements of order 3, such as $b = a^{11}$. (Note that

$$b = a^{11}, b^2 = (a^{11})^2 = a^{22}, b^3 = (a^{11})^3 = a^{33} = e.)$$

Now assume that G is not cyclic (there are no elements of order 33 in G). By Lagrange's theorem, the possible orders of elements are $1, 3, 11$. Suppose that there are no elements of order 3 in G. We will show that this leads to a contradiction, as follows. If there are no elements of order 3, then every element other than e has order 11. Since 11 is prime, by problem 9 above, if a, b are elements of order 11, then either $\langle a\rangle = \langle b\rangle$ or else $\langle a\rangle \cap \langle b\rangle = \{e\}$. Take any one element of order 11. We have 11 distinct elements of G in $\langle a\rangle$. Since there are 33 elements in G altogether, then there must be some $b \in G$ with $b \notin \langle a\rangle$. But as above, this implies $\langle a\rangle \cap \langle b\rangle = \{e\}$. This gives 10 additional elements in G in $\langle b\rangle$, but not in $\langle a\rangle$. However, $|G| = 33$, so there are still elements in G not in $\langle a\rangle \cup \langle b\rangle$. Let c be any one such element. Then $\langle c\rangle \cap \langle a\rangle = \{e\}$ and $\langle c\rangle \cap \langle b\rangle = \{e\}$. Thus $\langle c\rangle$ contains 10 additional elements of G other than e. But we still have additional elements G since $|\langle a\rangle \cup \langle b\rangle \cup \langle c\rangle| = 31$. However, now we get a contradiction, since if d is one of the elements of G not in the union of these three subgroups, then d must also have order 11. This is impossible since there are not 10 additional elements in G. Hence G must have some elements of order 3.

Section 7.6

5. (a) G is clearly nonempty. Let $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ be elements in G. Then

$$AB^{-1} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1/a' & -b'/(a'd') \\ 0 & 1/d' \end{pmatrix} = \begin{pmatrix} a/a' & (a'b - ab')/(a'd') \\ 0 & d/d' \end{pmatrix}.$$

Since $ad \neq 0$ and $a'd' \neq 0$, this matrix is also in G since $(a/a')(d/d') = (ad)/(a'd') \neq 0$. This shows that G is a subgroup of $\mathrm{GL}(2,\mathbb{R})$, hence a group itself.

Next, Consider N. N is closed under products:

$$\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b'\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & b+b'\\ 0 & 1\end{pmatrix} \in N,$$

and closed under inverses:

$$\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix} \in N.$$

Hence N is a subgroup of G.

(b) If $A = \begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \in G$ and $B = \begin{pmatrix}1 & b'\\ 0 & 1\end{pmatrix} \in N$, then

$$\begin{aligned} A^{-1}BA &= \begin{pmatrix}1/a & -b/(ad)\\ 0 & 1/d\end{pmatrix}\left(\begin{pmatrix}1 & b'\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\right)\\ &= \begin{pmatrix}1/a & -b/(ad)\\ 0 & 1/d\end{pmatrix}\begin{pmatrix}a & b+b'd\\ 0 & d\end{pmatrix}\\ &= \begin{pmatrix}1 & (b'd)/a\\ 0 & 1\end{pmatrix}. \end{aligned}$$

By definition, this is an element of N. By equivalent statement (2) in Theorem 7.34, this implies that N is a normal subgroup of G.

8. The group table for the quaternion group Q from problem 14 in Section 7.1 is:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(a) The cyclic subgroups of Q are:

$$\begin{aligned} \langle 1\rangle &= \{1\}\\ \langle -1\rangle &= \{1,-1\}\\ \langle i\rangle &= \{1,i,-1,-i\} = \langle -i\rangle\\ \langle j\rangle &= \{1,j,-1,-j\} = \langle -j\rangle\\ \langle i\rangle &= \{1,k,-1,-k\} = \langle -k\rangle \end{aligned}$$

(b) The cyclic subgroups $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$ are all normal by a result we proved in class, since they have order $4 = 8/2$. The other two cyclic subgroups are normal since $1, -1$ commute with all elements in Q, so $aH = Ha$ if $H = \{1\}$ or $H = \{1, -1\}$.

16. First, $K \cap N$ is a subgroup of G by the argument given in the solution for problem 9 from Section 7.5 above. Now we will show that $K \cap N$ is a normal subgroup of G by using equivalent statement (2) from Theorem 7.34. Let $g \in K \cap N$ and $a \in G$. Then $g \in K$ and $g \in N$. Since K is normal in G, we have $a^{-1}ga \in K$. Similarly, since N is normal in G, $a^{-1}ga \in N$. Therefore $a^{-1}ga \in K \cap N$. It follows that $a^{-1}(K \cap N)a \subset K \cap N$, so $K \cap N$ is a normal subgroup of G.

17. We will prove that $N \cap K$ is normal in K using the equivalent statement (2) of Theorem 7.34. So let $g \in N \cap K$ and let $a \in K$. Then $a^{-1}ga \in K$ because $a, g \in K$ and K is a subgroup. On the other hand, $a^{-1}ga \in N$ since $g \in N$, $a \in K \subseteq G$, and N is a normal subgroup of G. Hence $a^{-1}ga \in N \cap K$ whenever $g \in N \cap K$ and $a \in K$. Therefore $N \cap K$ is a normal subgroup of K.

22. This follows from the fact proved in Linear Algebra that $f(AB) = \det(AB) = \det(A)\det(B) = f(A)f(B)$.

23. Let $A \in \mathrm{SL}(2, \mathbb{R})$, so $\det(A) = 1$. If $B \in \mathrm{GL}(2, \mathbb{R})$ is an arbitrary invertible matrix, then by problem 22,

$$\det(B^{-1}AB) = \frac{1}{\det(B)} \det(A)\det(B) = \det(A) = 1.$$

Hence for all B,

$$B^{-1}\mathrm{SL}(2, \mathbb{R})B \subseteq \mathrm{SL}(2, \mathbb{R}).$$

Hence $\mathrm{SL}(2, \mathbb{R})$ is a normal subgroup of $\mathrm{GL}(2, \mathbb{R})$ by Theorem 7.34 (equivalent statement (2)).