Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 3
February 4, 2008

Section 8.4

6. Let $H \subseteq K$ be subgroups of G such that H is normal as a subgroup of K. This means that for all $x \in K$, $x^{-1}Hx = H$. By the definition, this means $x \in N(H)$, so $K \subseteq N(H)$.

7. (a) Let $A \subseteq G$ be a subgroup. Let $x \in A$. Then $x^{-1}Ax \subseteq A$ since A is closed under inverses and products. On the other hand if $y \in A$ is an arbitrary element, then $xyx^{-1} \in A$ since A is a subgroup and hence $x^{-1}(xyx^{-1})x = y \in x^{-1}Ax$. Therefore $A \subseteq x^{-1}Ax$, so combining the two inclusions, $A = x^{-1}Ax$. This shows $A \subset N(A)$.

(b) We have

$$\begin{aligned} g \in N(A) &\iff g^{-1}Ag = A \quad \text{by definition} \\ &\iff Ag = gA \quad \text{(multiply by } g \text{ on left)}. \end{aligned}$$

12. Let K be a Sylow p-subgroup of G, and N be a normal subgroup of G. Assume that K is a normal subgroup of N. We claim first that this means that K is also a Sylow p-subgroup of N. Assume $|G| = p^t m$ with $(p, m) = 1$, so $|K| = p^t$. But by Lagrange's theorem, $|N|$ divides $|G|$, and so the largest power of p that can divide N is p^t. Since $K \subseteq N$, we must have $|N| = p^t m'$ where $(p, m') = 1$, and hence K is also a Sylow p-subgroup of G. Now let x be any element of G. Since N is normal in G, $x^{-1}Nx = N$. Since $K \subseteq N$, this implies $x^{-1}Kx \subseteq N$. But since $|x^{-1}Kx| = |K|$, it follows that $x^{-1}Kx = K$ is also a Sylow p-subgroup of N. Since K is normal in N, Sylow 2 implies that there is just one such Sylow p-subgroup of N, namely K. This means that $x^{-1}Kx = K$. Therefore, K is also normal in G.

Section 8.5

1. We have $|G| = p^2 q$ with p, q prime, $p < q$ and $q \not\equiv 1 \bmod p$. The only hypothesis we are missing to apply Theorem 8.30 is the one that says $p^2 \not\equiv 1 \bmod q$. Suppose that $q|(p^2 - 1)$. Then since q is prime, $q|(p + 1)$ or $q|(p - 1)$. The second is impossible since $p < q$ so $p - 1 < q$ as well. The first is also impossible. Suppose that $q|(p + 1)$. There are two cases to consider. First, if $p = 2$, then $q = 3$ and this contradicts $q \not\equiv 1 \bmod p$. Second, if p is an odd prime, then $p + 1$ is even, $p + 1 = 2\ell$ for some $\ell < p$. It must be the case that $q|\ell$ since $q > p$, so q is also an odd prime. But this is also impossible since $p < q$. Hence the hypothesis for Theorem 8.30 is satisfied, and G must be abelian.

6. The n for which these theorems are sufficient are

Theorem 7.28 (prime order)	applies to	$n = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$
	applies to	$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$
Corollary 8.29 (order p^2)	applies to	$n = 4, 9, 25, 49$
Theorem 8.33 (order $2p$)	applies to	$n = 6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86, 94$
Corollary 8.18 (order pq)	applies to	$n = 15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95$
Theorem 8.30 (order p^2q)	applies to	$n = 45, 99$
Theorem 8.34 (order 8)	applies to	$n = 8$
Theorem 8.35 (order 12)	applies to	$n = 12$
none of these	apply to	$n = 16, 18, 20, 21, 24, 27, 28, 30, 32, 36, 39,$
		$40, 42, 44, 48, 50, 52, 54, 55, 56, 57, 60, 63$
		$64, 66, 68, 70, 72, 75, 76, 78, 80, 81, 84, 88$
		$90, 92, 93, 96, 98, 100.$

8. (a) We have

$$\begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pm 1 & a \pm b \\ 0 & 1 \end{pmatrix}.$$

Moreover,

$$\begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \pm 1 & \mp a \\ 0 & 1 \end{pmatrix}$$

Hence this set of matrices is closed under products and inverses and forms a subgroup of $\mathrm{GL}(2, \mathbb{Z}_n)$.

(b) Let $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $R^n = I$ (the identity matrix). Similarly let $D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ so $D^2 = I$. We have

$$DR = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = R^{-1}D.$$

Therefore the mapping given by $R^iD^j \mapsto r^id^j$ is an isomorphism from this group of matrices to D_n.

10. We have $D_n = \langle r, d : d^n = e, r^2 = e, dr = r^{-1}d \rangle$, and every element can be written uniquely as r^id^j with $0 \le i \le n-1$ and $0 \le j \le 1$. (a) If $n = 2k$, then $r^ir^k = r^{i+k} = r^kr^i$, so r^k commutes with all the elements of the subgroup generated by r. Moreover, applying the relation $dr = r^{-1}d$ repeatedly,

$$(r^id)r^k = r^i(dr^k) = r^i(r^{-1})^kd = r^i(r^k)^{-1}d = (r^ir^k)d = (r^kr^i)d = r^k(r^id).$$

Therefore $r^k \in Z(D_n)$.

(b) We show that every other element of D_n besides e, r^k does not commute with something, which will imply that $Z(D_n) = \{e, r^k\}$. Consider the elements r^i for $i \neq 0, k$ first. We have $dr^i = (r^{-1})^i d = (r^i)^{-1} d = r^{n-i} d$. Since $i \neq k$, $i \not\equiv n - i \bmod n$, and this shows that $r^i \notin Z(D_n)$. Similarly, the element $r^i d$ does not commute with r:

$$(r^i d)r = r^i(dr) = r^i r^{-1} d = r^{i-1} d \quad \text{but} \quad r(r^i d) = r^{i+1} d.$$

Therefore $r^i d \notin Z(D_n)$ for all i.

(c) The same reasoning as in part (b) shows that when n is odd, $Z(D_n) = \{e\}$ since there is no element such that $(r^i)^{-1} = r^i$ except $r^0 = e$.

11. By consulting the group table, $Z(Q) = \{1, -1\}$.