Kris Harper
MATH 25700
Homework 3 October 16, 2009

Problem 1 (2.1.3). *Show that the following subsets of the dihedral group D_8 are actually subgroups:*
(a) $\{1, r^2, s, sr^2\}$
(b) $\{1, r^2, sr, sr^3\}$.

Proof. (a) Obviously $H = \{1, r^2, s, sr^2\}$ is nonempty. Since H is finite, we need only check that H is closed under multiplication. For r^2 we have $r^2r^2 = r^4 = 1$, $r^2s = sr^{-2} = sr^2 \in H$, and $r^2(sr^2) = (sr^{-2})r^2 = s \in H$. For s we have $sr^2 \in H$, $s^2 = 1$ and $s(sr^2) = s^2r^2 = r^2 \in H$. Finally for sr^2 we have $sr^2r^2 = sr^4 = s \in H$, $sr^2s = s^2s^{-2} = r^2 \in H$ and $sr^2sr^2 = s^2r^{-2}r^2 = 1$. Thus H is a subgroup of D_8 since it's finite, nonempty and is closed under multiplication.

(b) By a similar argument as above, we only need to check that $H = \{1, r^2, sr, sr^3\}$ is closed under multiplication. For r^2 we have $r^2r^2 = 1$, $r^2sr = sr^{-2}r = sr^2r = sr^3 \in H$, and $r^2sr^3 = sr^{-2}r^3 = sr \in H$. For sr we have $srr^2 = sr^3 \in H$, $srsr = ssr^{-1}r = 1 \in H$ and $srsr^3 = ssr^{-1}r^3 = ssr^2 = r^2 \in H$. Finally for sr^3 we have $sr^3r^2 = sr^5 = sr \in H$, $sr^3sr = ssr^{-3}r = ssr^2 = r^2 \in H$ and $sr^3sr^3 = ssr^{-3}r^{-3} = 1$. Thus H is a subgroup of D_8 since it's finite, nonempty and is closed under multiplication. $\square$

Problem 2 (2.1.6). *Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the* torsion subgroup *of G). Give an explicit example where this set is not a subgroup when G is non-abelian.*

Proof. Clearly $|1| = 1 < \infty$ so $H = \{g \in G \mid |g| < \infty\} \neq \emptyset$. Take $x, y \in H$ such that $|x| = n$ and $|y| = m$. Note that this implies $|y^{-1}| = m$ since $y^m = 1$ and we can multiply by $y^{-m} = (y^{-1})^m$ on both sides. Now since G is abelian we have $(xy^{-1})^{nm} = x^{nm}(y^{-1})^{nm} = (x^n)^m((y^{-1})^m)^n = 1$. Therefore $|xy^{-1}| \leq nm < \infty$. This shows that H is a subgroup of G.

As an example, consider the group with presentation $\langle r, s \mid s^2 = 1, rs = sr^{-1}\rangle$. This is a nonabelian group with infinite order. Note that $|r| = \infty$, $|s| = 2$, $|sr| = 2$. But $(s)(sr) = s^2r = r$ so $|(s)(sr)| = \infty$. $\square$

Problem 3 (2.1.10). *(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.*
(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Proof. (a) Since $1 \in H$ and $1 \in K$ we know $H \cap K \neq \emptyset$. Now take $x, y \in H \cap K$. Note that this means $x, y \in H$ and $x, y \in K$. But since $H \leq G$ we know $xy^{-1} \in H$ and the same for K. Therefore $xy^{-1} \in H \cap K$ and we're done.

(b) Let $\mathcal{A}$ be a nonempty collection of subgroups of G indexed by some set I. Note that $\bigcap_{i \in I} A_i \neq \emptyset$ since $1 \in A_i$ for all $i \in I$. Now consider $x, y \in \bigcap_{i \in I} A_i$. This means $x, y \in A_i$ for each $i \in I$. But since $A_i \leq G$ we have $xy^{-1} \in A_i$ for each $i \in I$. Then this means that $xy^{-1} \in \bigcap_{i \in I} A_i$. Therefore $\bigcap_{i \in I} A_i$ is a subgroup of G by the subgroup criterion. $\square$

Problem 4 (2.1.15). *Let $H_1 \leq H_2 \leq \ldots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.*

Proof. Clearly $\bigcup_{i=1}^{\infty} H_i \neq \emptyset$ since $1 \in H_1$. Let $x, y \in \bigcup_{i=1}^{\infty} H_i$. Then $x \in H_i$ and $y \in H_j$ for some i, j. Without loss of generality suppose $i \leq j$. Then we know $H_i \leq H_j$ and so $x, y \in H_j$. Since $H_j \leq G$, we know $xy^{-1} \in H_j$ and thus $xy^{-1} \in \bigcup_{i=1}^{\infty} H_i$. Therefore $\bigcup_{i=1}^{\infty} H_i \leq G$. $\square$

Problem 5 (2.1.16). *Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0$ for all $i > j\}$ is a subgroup of $GL_n(F)$ (called the group of upper triangular matrices).*

Proof. Let $H = \{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$. The identity matrix $I \in H$ since $I_{ij} = 0$ for all $i \neq j$. Take $X, Y \in H$. Note that $Y^{-1} \in H$ because the inverse of an upper triangular matrix is an upper triangular matrix. This fact can be established with contradiction as multiplying an upper-triangular matrix by one which is not upper triangular will always result in an off-diagonal nonzero element. Furthermore, consider $(XY^{-1})_ij = \sum_{k=1}^{n} X_{ik}Y_{kj}$. Note that $X_{ik} = 0$ whenever $i > k$, and $Y_{kj} = 0$ whenever $k > j$.

Therefore, provided that $i > j$, this sum is always 0. This then shows that XY^{-1} is an upper triangular matrix. Therefore $XY^{-1} \in H$ and $H \leq GL_n(F)$. □

Problem 6 (2.1.17)**.** *Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0$ for all $i > j$ and $a_i i = 1$ for all $i\}$ is a subgroup of $GL_n(F)$*

Proof. As in Problem 5 we see that $I \in H$. Let $X, Y \in H$. The fact that for $X, Y \in H$ we have $XY^{-1} \in H$ is the same proof as in Problem 5. □

Problem 7 (2.2.6)**.** *Let H be a subgroup of the group G.*
(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.
(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. (a) Since $H \leq G$ we know that H is closed under inverses and products and $H \neq \emptyset$. To show $H \leq N_G(H)$ we must show that $H \subseteq N_G(H)$. Let $x \in H$. Consider xhx^{-1} for some $h \in H$. Since H is closed under products and inverses, we know that $xhx^{-1} \in H$. Furthermore, for $h \in H$ we know $xhx^{-1} \in H$. We thus have $xHx^{-1} = H$, and therefore $x \in N_G(H)$. Hence, $H \subseteq N_G(H)$ and since it respects the group operation, $H \leq N_G(H)$.

As an example, take any set H which doesn't contain the identity. Since $1 \cdot H \cdot 1^{-1} = H$ we know $1 \in N_G(H)$, but it's clear that $H \not\leq N_G(H)$ since $1 \notin H$.

(b) Suppose $H \leq C_G(H)$. Then for $x, y \in H$ we know $xyx^{-1} = y$ which implies $xy = yx$. Conversely, suppose H is abelian. Then for all $x, y \in H$ we have $xy = yx$ and so $xyx^{-1} = y$. But $C_G(H) = \{x \in G \mid xyx^{-1} = y \text{ for all } y \in H\}$. This shows that $H \subseteq C_G(H)$. Since $H \leq G$ we know $H \leq C_G(H)$. □

Problem 8 (2.2.7)**.** *Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:*
(a) $Z(D_{2n}) = 1$ if n is odd.
(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Proof. (a) We know that $s \notin Z(D_{2n})$ since $rs = sr^{-1}$. Take $r^k \in D_{2n}$ for $k \neq 0$. Note that $r^k \neq r^-k$, otherwise $r^{2k} = 1 = r^n$ and n is even. Therefore $r^k s = sr^{-k}$ shows that r^k doesn't commute with s. Thus the only element which commutes with all elements of D_{2n} is 1 and $Z(D_{2n}) = 1$.

(b) From Problem 1.2.4 we know that since $n = 2k$, r^k is the only nonidentity element which commutes with every element of D_{2n}. Therefore $Z(D_{2n}) = \{1, r^k\}$. □

Problem 9 (2.2.8)**.** *Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.*

Proof. Note that σ is a group action acting on the set $\{1, \ldots, n\}$ such that $\sigma.i = \sigma(i)$. It's easy to see that this is indeed a group action. Since the stabilizing set of a group action is always a subgroup of the acting group, we know that $G_i \leq G$. In any permutation of $\{1, 2, \ldots, n\}$ there are n possibilities for the location of i. Since G_i is the set of permutations which fix i, we see that $|G_i| = |S_n|/n = (n-1)!$. □

Problem 10 (2.2.9)**.** *For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).*

Proof. Let $h \in N_H(A)$. Then $hAh^{-1} = A$ and $h \in H$. But since $h \in G$ this means that $h \in N_G(A)$. Moreover, $h \in H$ as well which means $h \in N_G(A) \cap H$. For the other inclusion, suppose $h \in N_G(A) \cap H$. Then $hAh^{-1} = A$. But since $h \in H$ we know that $h \in N_H(A)$. Both inclusions show that $N_H(A) = N_G(A) \cap H$. Since $N_H(A) \subseteq N_G(A) \cap H$ it follows that $N_H(A) \subseteq H$. Because of this fact, we know that $N_H(A)$ is closed under inverses and products. Therefore $N_H(A) \leq H$. □

Problem 11 (2.3.11)**.** *Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.*

Proof. We've shown that the groups $\langle r \rangle$ and $\langle s \rangle$ are cyclic subgroups of D_{2n}. Additionally, $\langle r^2 \rangle$ is a subgroup as per Problem 8. Consider the powers of r multiplied by s. We have $(r^k s)(r^k s) = r^k r^{-k} s^2 = 1$. This covers all the possible cyclic groups so we are left with $\langle 1 \rangle$, $\langle r \rangle$, $\langle r^2 \rangle$, $\langle s \rangle$, $\langle rs \rangle$, $\langle r^2 s \rangle$, $\langle r^3 s \rangle$. Consider the subgroup $\{1, s, r^2, sr^2\}$. From Problem 1 we know this is a subgroup. □

Problem 12 (2.3.12). *Prove that the following groups are* not *cyclic:*
(a) $Z_2 \times Z_2$.
(b) $Z_2 \times \mathbb{Z}$.
(c) $\mathbb{Z} \times \mathbb{Z}$.

Proof. (a) We can write this group as $\{1, a, b, c\}$ such that $a^2 = b^2 = c^2 = 1$ and $ab = c$, $ac = b$ and $bc = a$. To see the identification, take $1 = (0, 0)$, $a = (1, 0)$, $b = (0, 1)$ and $c = (1, 1)$. The necessary equalities hold. Note that each element has order 1 or 2, but $|Z_2 \times Z_2| = 4$ and therefore it is not cyclic.

(b) We can write $Z_2 \times \mathbb{Z} = \langle (0, 1), (1, 0) \rangle$. If we take some element $(a, b) \in Z_2 \times \mathbb{Z}$ then we can write this as $a(1, 0) + b(0, 1)$. This then implies that $Z_2 \times \mathbb{Z}$ is not cyclic.

(c) As in part (b) write $\mathbb{Z} \times \mathbb{Z} = \langle (0, 1), (1, 0) \rangle$. The same linear decomposition from (b) works here. Therefore $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. □

Problem 13 (2.3.16). *Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do* not *commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of x and y.*

Proof. Let l be the least common multiple of n and m such that $an = l$ and $bm = l$. Then $1 = (x^n)^a (y^m)^b = x^{an} y^{bm} = x^l y^l = (xy)^l$ since x and y commute. But we know that if $|xy| = k$ then $|(xy)^l| = k/(k, l)$. Since $(xy)^l = 1$ we have $k = (k, l)$ and in particular $k \mid l$.

In the case of D_6 we have $|r| = 3$ and $|s| = 2$. The least common multiple of 2 and 3 is 6. But $(rs)(rs) = rr^{-1}s^2 = 1$, so $|rs| = 2$. Thus if x and y do not commute, the statement is false. In D_6 consider the commuting elements r and r^2. We know $|r| = 6$ and $|r^2| = 3$ so the least common multiple is 6. But $rr^2 = r^3$ and $|r^3| = 2$. Nevertheless, $2 \mid 6$. □

Problem 14 (2.3.26). *Let Z_n be a cyclic group of order n and for each integer a let*

$$\sigma_a : Z_n \to Z_n \text{ by } \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.
(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.
(c) Prove that every *automorphism of Z_n is equal to σ_a for some integer a.*
(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\phi(n)$).

Proof. (a) Note that if $|x| = n$ then $Z_n = \langle x^a \rangle$ if and only if $(a, n) = 1$. Suppose that σ_a is an automorphism of Z_n. Then for each $y \in Z_n$ there exists $x \in Z_n$ such that $\sigma_a(x) = x^a = y$. There exists $y \in Z_n$ such that $|y| = n$ and so $Z_n = \langle y \rangle = \langle x^a \rangle$. But the above theorem states that $(a, n) = 1$. Conversely, suppose that $(a, n) = 1$. Then we know $Z_n = \langle x^a \rangle$. This shows that σ_a is surjective. To show that it's injective, take $y^i, y^j \in Z_n$ with $y^i \neq y^j$. Then we have $\sigma_a(y^i) = (y^a)^i \neq (y^a)^j = \sigma_a(y^j)$. The fact that σ_a is a homomorphism follows from $\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$. Thus, σ_a is an automorphism.

(b) Suppose $\sigma_a = \sigma_b$. Then for all $x \in Z_n$ we have $x^a = x^b$ and $x^{a-b} = 1$. For some x, $|x| = n$, so we have $n \mid (a - b)$ which means $a \equiv b \pmod{n}$. Conversely, suppose that $a \equiv b \pmod{n}$. Then $n \mid (a - b)$ so there exists c such that $cn = a - b$. Then $1 = (x^n)^c = x^{cn} = x^{a-b}$. Therefore $x^a = x^b$ and so $\sigma_a = \sigma_b$.

(c) Let $\varphi : Z_n \to Z_n$ be an automorphism. Then since elements of Z_n are of the form x^k for $1 \leq k \leq n$ we know $\varphi(x) = x^k$ for some k. But then note that

$$\varphi(x^j) = \varphi(x \cdot x \cdot \cdots \cdot x) = \varphi(x)\varphi(x) \ldots \varphi(x) = (\varphi(x))^j = (x^k)^j = (x^j)^k.$$

Thus $\varphi = \sigma_k$.

(d) We have

$$\sigma_a \circ \sigma_b(x) = \sigma_a(\sigma_b(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x).$$

Let $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}(Z_n)$ be the map described. Part (b) shows injectivity of φ. Part (c) shows surjectivity. And the above calculation shows that the group structure is preserved. Thus, φ is an isomorphism. □

Problem 15 (2.4.14)**.** *A group H is called* finitely generated *if there is a finite set A such that $H = \langle A \rangle$.*
(a) Prove that every finite group is finitely generated.
(b) Prove that $\mathbb{Z}$ is finitely generated.
(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.

Proof. (a) Let $H = \{1, a_1, a_2, \ldots, a_n\}$ be a finite group. Then $H = \langle a_1, a_2, \ldots, a_n \rangle$.

(b) Let $n \in \mathbb{Z}$. Then we can write $n = \pm 1 \cdot n$. Therefore $\mathbb{Z} = \langle 1 \rangle$.

(c) Let $H = \langle a_1/b_1, a_2/b_2, \ldots, a_n/b_n \rangle$ be a finitely generated additive subgroup of $\mathbb{Q}$. Let $x = \prod_{i=1}^n b_i$. Now take $m_1/n_1 = \sum_{j=k}^{l} a_{i_j}/b_{i_j}$ and $m_2/n_2 = \sum_{j=k'}^{l'} a_{i_j}/b_{i_j}$. Note that $n_1 = \prod_{j=k}^{l} b_{i_j}$ and $n_2 = \prod_{j=k'}^{l'} b_{i_j}$. Now consider the sum $(m_1n_2 + m_2n_1)/(n_1n_2)$. Note that if any terms in the products n_1 and n_2 coincide, then we can undistribute them in the sum in the numerator and cancel them with the denominator. This shows that $n_1n_2 \mid x$. Letting $y = x/(n_1n_2)$ we have $1 \cdot (m_1/n_1 + m_2/n_2) = (y/y)(m_1/n_1 + m_2/n_2) = (y(m_1n_2 + m_2n_1))/(yn_1n_2) = (ym_1n_2 + ym_2n_1)/x$. We have thus shown that $H \leq \langle 1/x \rangle$ which proves that H is cyclic. □

Problem 16 (2.4.16)**.** *A subgroup M of a group G is called a* maximal subgroup *if $M \neq G$ and the only subgroups of G which contain M are M and G.*
(a) Prove that H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.
(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.
(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup of H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Proof. (a) If H is maximal then we're done. If H is not maximal, then since $H \neq G$, there must be a subgroup H_1 of smallest order which contains H. If $H_1 = G$ then H must have been maximal since H and G both contain H and since H_1 is of smallest order, there are no other such subgroups. Otherwise, if H_1 is maximal then we're finished, and if not then there exists a subgroup H_2 of smallest order which contains H_1. Since G is finite, this process must eventually stop so that $H_i = G$ for some i. Then H_{i-1} is maximal since is a proper subgroup of G for which the only subgroups which contain it are H_{i-1} and G.

(b) Clearly $\langle r \rangle \neq D_{2n}$ since $s \notin \langle r \rangle$. Let $H \leq D_{2n}$ be a subgroup such that $\langle r \rangle \leq H$. Since all powers of r are already in H, we must have $sr^k \in H$ or $r^k s \in H$. Note that if $sr^k \in H$ then $sr^k r^{-k} = s \in H$. A similar argument holds for $r^k s$. Therefore $s \in H$, and so $H = D_{2n}$. This shows that $\langle r \rangle$ is maximal in D_{2n}.

(c) Let H be a maximal subgroup of G. Note that since G is cyclic, there is a unique cyclic subgroup $\langle x^d \rangle$ of order a for each $a \mid n$ where $ad = n$. Furthermore, H is one of these subgroups. If $H = \langle x^a \rangle$ for $a = bc$ then $H = \langle x^{bc} \rangle = \langle (x^b)^c \rangle$. Therefore $H \leq \langle x^b \rangle$. But since H is maximal, $H = \langle x^p \rangle$ where p is not the product of two integers. Therefore p is prime.

Conversely, suppose that $H = \langle x^p \rangle$ for some prime p dividing n. Then let $K \leq G$ be a subgroup such that $H \leq K$. By the statement above, we know $K = \langle x^a \rangle$ where a divides n. Since $H \leq K$ we know that $x^p = (x^a)^k = x^{ak}$ for some k. If $k \neq 1$ then p is not prime, so $k = 1$. But then $p = a$ and $H = K$. Furthermore, we know H has order n/p and since $p \neq 1$ we see $H \neq G$. This shows that H is maximal. □

Problem 17 (2.4.17)**.** *Let G be a finitely generated group, say $G = \langle g_1, g_2, \ldots, g_n \rangle$ and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let $\mathcal{C}$ be a chain in $\mathcal{S}$.*
(a) Prove that the union, H, of all the subgroups in $\mathcal{C}$ is a subgroup of G.
(b) Prove that H is a proper *subgroup.*
(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Proof. (a) Since $\mathcal{S}$ is partially ordered by inclusion, this follows directly from Problem 4.

(b) Suppose that $H = G$. Then for each i, $g_i \in H$. But then each g_i is in a proper subgroup of G lying in $\mathcal{C}$. But since $\mathcal{C}$ is chain, each subgroup is contained in another in $\mathcal{C}$. Since there are only finitely many g_i, there must be one subgroup which contains all of them. But then this subgroup isn't proper. This is a contradiction and so H must be a proper subgroup.

(c) Part (b) shows that $H \in \mathcal{S}$ and part (a) shows that H is an upper bound for $\mathcal{C}$. Since $\mathcal{S}$ is nonempty ($\langle 1 \rangle \in \mathcal{S}$) and each chain has an upper bound, by Zorn's Lemma $\mathcal{S}$ must have a maximal element. $\square$

Problem 18 (2.5.7)**.** *Find the center of D_{16}.*

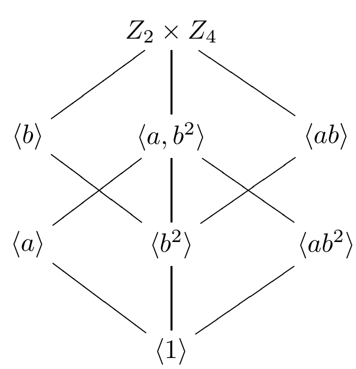
Proof. From Problem 8 we know that $Z(D_{16}) = \{1, r^4\}$. $\square$

Problem 19 (2.5.8)**.** *In each of the following groups, find the normalizer of each subgroup:*
(a) S_3.
(b) Q_8.

Proof. (a) The subgroups of S_3 are $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 2)\rangle$ and $\langle(1\ 2\ 3)\rangle$. We know $(1\ 2\ 3) \notin N_{S_3}(\langle(1\ 2)\rangle)$ because $\langle(1\ 2)\rangle = \{(1), (1\ 2)\}$ and $(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (1\ 2\ 3)^2(1\ 2) \notin N_{S_3}(\langle(1\ 2)\rangle)$. The same argument holds for $(1\ 2\ 3)^2$. Now consider $(1\ 3)$. We see that $(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3) \notin \langle(1\ 3)\rangle$. The same argument holds for $(2\ 3)$. This shows that $N_{S_3}(\langle(1\ 2)\rangle) = \langle(1\ 2)\rangle$. A similar statement holds for $\langle(1\ 3)\rangle$ and $\langle(2\ 3)\rangle$. Now note that $\langle(1\ 2\ 3)\rangle \leq N_{S_3}(\langle(1\ 2\ 3)\rangle) \leq S_3$. Since S_3 has order 6 and $\langle(1\ 2\ 3)\rangle$ has order 3, from Lagrange's Theorem we know that $N_{S_3}(\langle(1\ 2\ 3)\rangle)$ is either $\langle(1\ 2\ 3)\rangle$ or S_3. Noting that $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 2\ 3)^{-1}$ and that a similar statement can be said for $(1\ 2\ 3)^2$, we see that $(1\ 2) \in N_{S_3}(\langle(1\ 2\ 3)\rangle)$. Since $(1\ 2) \notin \langle(1\ 2\ 3)\rangle$ we must have $N_{S_3}(\langle(1\ 2\ 3)\rangle) = S_3$. A similar proof shows the same is true for $(1\ 2\ 3)^2$. This delineates all the normalizers for subgroups of S_3.

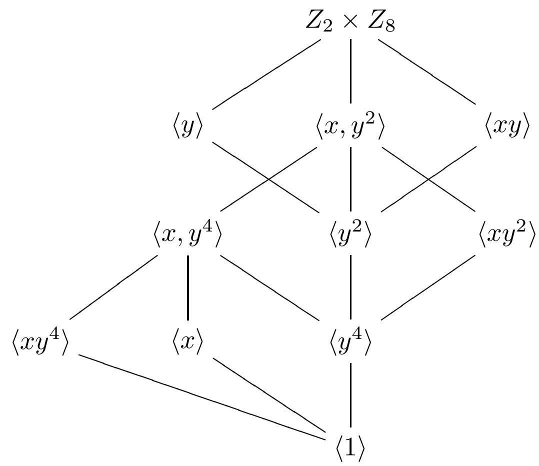
(b) From Problem 25 we know that every subgroup of Q_8 is normal. This is equivalent to saying $N_{Q_8}(H) = Q_8$ for $H \leq Q_8$. $\square$

Problem 20 (2.5.12)**.** *The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.*



Kris Harper
MATH 25700
Homework 3 October 16, 2009

Problem 21 (2.5.13). *The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, $\langle y \rangle \cong Z_8$ and $\langle xy \rangle \cong Z_8$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of G, giving each subgroup in terms of at most two generators.*

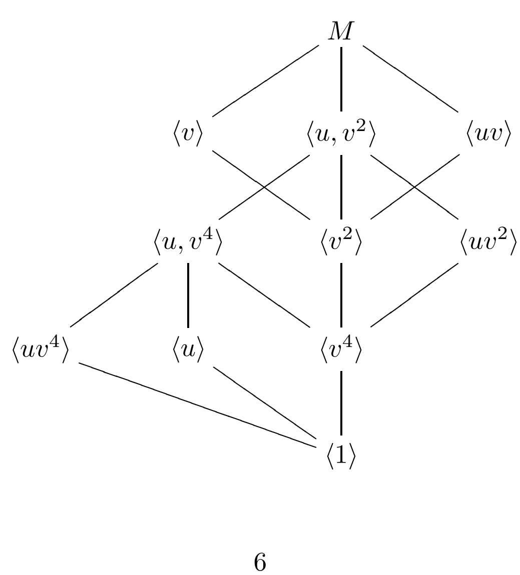


Problem 22 (2.5.14). *Let M be the group of order 16 with the following presentation:*

$$\langle u, v \mid u^2 = v^8 = 1, uv = uv^5 \rangle$$

(sometimes called the modular *group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle$, $\langle v \rangle$ and $\langle uv \rangle$ and every proper subgroup is contained in one of these three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, $\langle v \rangle \cong Z_8$ and $\langle uv \rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ but that these two groups are not isomorphic.*

Proof. Let $G = \langle u, v^2 \rangle$ and $H = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$. Let $\varphi : H \to G$ be a function such that $\varphi(a) = u$ and $\varphi(b) = v^2$. Comparing the two sets quickly shows that φ is a bijection (the two sets are identical with $v^2 = b$). Now take $\varphi(ab) = uv^2 = \varphi(a)\varphi(b)$. This shows that the two sets are isomorphic. It should be immediately obvious that $\langle v \rangle \cong Z_8$ since this *is* the cyclic group of order 8. To show $\langle uv \rangle \cong Z_8$ we need only show that $|uv| = 8$. But this is easily seen since $|v| = 8$ and $|u| \mid |v|$. Note that $M \not\cong Z_2 \times Z_8$ because M is not abelian. That is, if $\varphi : Z_2 \times Z_8 \to M$ is an isomorphism, then $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \phi(b)\phi(a)$. But this is not in general true for M. Therefore $M \not\cong Z_2 \times Z_8$. The lattice for M is



□

Problem 23 (3.1.3)**.** *Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a nonabelian group G containing a proper normal subgroup N such that G/N is abelian.*

Proof. Let $xB, yB \in A/B$. Since $xy = yx$ we see that $xByB = (xy)B = (yx)B = yBxB$. Consider $G = Q_8/\langle i\rangle$. From Problem 25 we know that $G \cong \mathbb{Z}/2\mathbb{Z}$, which is abelian, while $\langle i\rangle \subsetneq Q_8$. □

Problem 24 (3.1.22)**.** *(a) Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.*

Proof. Let $g \in G$. Since $gHg^{-1} = H$ and $gKg^{-1} = K$, consider

$$g(H\cap K)g^{-1} = \{gxg^{-1} \mid x \in H, x \in K\} = \{gxg^{-1} \mid x \in H\} \cap \{gxg^{-1} \mid x \in K\} = gHg^{-1} \cap gKg^{-1} = H \cap K.$$

Since H and K are normal subgroups of G, we have $gHg^{-1} \subseteq H$. □

Problem 25 (3.1.32)**.** *Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient.*

Proof. The subgroups of Q_8 are $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, $\langle -1\rangle$, $\langle 1\rangle$. Consider $\langle i\rangle = \{1, i, -1, -i\}$ and the coset $j\langle i\rangle = \{jx \mid x \in \langle i\rangle\}$. Note that $j(1) = (1)j$, $ji = -ij$, $j(-1) = (-1)j$ and $j(-i) = ij$. Therefore $j\langle i\rangle = \langle i\rangle j$. A similar argument holds for $\langle j\rangle$ and $\langle k\rangle$ since these groups have identical structures to $\langle i\rangle$. Also note that $i\langle -1\rangle = \langle -1\rangle$ since $i(1) = (1)i$ and $i(-1) = (-1)i$. A similar argument holds for $j\langle -1\rangle$ and $k\langle -1\rangle$. This shows that for every subgroup of Q_8, the left coset is also a right coset. Thus, every subgroup is normal.

For $Q_8/\langle i\rangle$ we have

$$j\langle i\rangle = \{j, ji, -ji, -j\} = \{j, -k, k, -j\} = \{ki, -k, k, -ki\} = k\langle i\rangle.$$

Also since every element $x \in \langle i\rangle$ appears as both x and $-x$ we now know $\pm j\langle i\rangle = \pm k\langle i\rangle$. Likewise

$$i\langle i\rangle = \{i, i^2, -i, -i^2\} = \{i, 1, -i, -1\} = 1\langle i\rangle$$

and the same argument above shows that $\pm i\langle i\rangle = \pm 1\langle i\rangle$. Thus, we can take $j\langle i\rangle$ and $\langle i\rangle$ to be the two elements of $Q_8/\langle i\rangle$. Note that $j\langle i\rangle \cdot j\langle i\rangle = -\langle i\rangle = \langle i\rangle$. Thus we have $Q_8/\langle i\rangle \cong \mathbb{Z}/2\mathbb{Z}$. This same argument holds for $Q_8/\langle j\rangle$ and $Q_8/\langle j\rangle$ as well.

For $Q_8/\langle -1\rangle$ we have $\pm\langle -1\rangle = \{1, -1\}$. Thus for $x \in \{i, j, k\}$ we also have $\pm x\langle -1\rangle = \{x, -x\}$. Therefore $(\pm i\langle -1\rangle)^2 = (\pm j\langle -1\rangle)^2 = (\pm k\langle -1\rangle)^2 = \pm\langle -1\rangle$. Furthermore, $i\langle -1\rangle \cdot j\langle -1\rangle = -k\langle -1\rangle = k\langle -1\rangle$. Since similar statements can be said about jk and ki, we see that $Q_8/\langle -1\rangle \cong V_8$, the Klein-4 group. □

Problem 26 (3.2.1)**.** *Which of the following are permissible orders for subgroups of a group of order* 120*:* 1*,* 2*,* 5*,* 7*,* 9*,* 15*,* 60*,* 240*? For each permissible order, give the corresponding index.*

Proof. By Lagrange's Theorem we know that permissible orders are those which divide 120. Therefore, the permissible orders are 1, 2, 5, 15, and 60 with indices 120, 60, 24, 8 and 2 respectively. □

Problem 27 (3.2.5)**.** *Let H be a subgroup of G and fix some element $g \in G$.*
(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.
(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n, then $H \trianglelefteq G$.

Proof. (a) Since $1 \in H$ we know $1 = g \cdot 1 \cdot g^{-1} \in gHg^{-1}$ and so the set is nonempty. Take $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for $h_1, h_2 \in H$. Also $y^{-1} = (g^{-1})^{-1}(gh_2)^{-1} = gh_2^{-1}g^{-1}$. Therefore $xy^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2^{-1}g^{-1}$. Since H is a subgroup of G we know $h_1h_2^{-1} \in H$ and thus $xy^{-1} \in gHg^{-1}$. This shows that $gHg^{-1} \leq G$. Now suppose that $x = y$ so that $gh_1g^{-1} = gh_2g^{-1}$. Then $h_1 = h_2$. Also, if $x \in gHg^{-1}$ then there's clearly $h_1 \in H$ for which $x = ghg^{-1}$. Thus the map $\phi : H \to gHg^{-1}$ where $h \mapsto ghg^{-1}$ is a bijection. Thus $|H| = |gHg^{-1}|$.

(b) If H is the unique subgroup of order n of G then from part (a) we know that $gHg^{-1} = H$ for all $g \in G$. This shows that $H \trianglelefteq G$. □

Problem 28 (3.2.8)**.** *Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.*

Proof. Suppose to the contrary that $x \in H \cap K$ with $x \neq 1$. Then $\langle x \rangle \leq H$ and $\langle x \rangle \leq K$. But since $x \neq 1$ we know that $|\langle x \rangle| = k$ for some $k \neq 1$. Therefore each of H and K have a subgroup of order k. By Lagrange's Theorem we have $k \mid |H|$ and $k \mid |K|$ contradicting the fact that $(|H|, |K|) = 1$. □