MATH1530, HOMEWORK 4

Section 2.2

2. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

By definition, $C_G(Z(G)) = \{g \in G : gag^{-1} = a \text{ for all } a \in Z(G)\}$. But if $a \in Z(G)$, again by definition, $ga = ag$ for all $g \in G$, or equivalently $gag^{-1} = a$ for all g. That is, any $g \in G$ is contained in $C_G(Z(G))$ showing that $C_G(Z(G)) = G$.

Then since $C_G(A) \leq N_G(A)$, $G \leq N_G(Z(G)) \leq G$ implies $N_G(Z(G)) = G$.

4. For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group.

For any group, it is trivial that $C_G(e) = G$. Now for any $x \in G$, notice that $C_G(x) \supseteq \{...x^{-2}, x^{-1}, e, x, x^2, ...\}$, since $x^i x x^{-i} = x$ for any $i \in \mathbb{Z}$. Indeed, it is also true that $C_G(x^i) \supseteq \{...x^{-2}, x^{-1}, e, x, x^2, ...\}$ for the same reason. And we prove that the center $Z(G)$ equals the intersection of all $C_G(g)$ where $g \in G$.

Claim. $Z(G) = \cap_{h \in G} C_G(h)$.

Proof. Let $g \in Z(G)$. Then $ghg^{-1} = h$ for all $h \in G$, which implies $g \in C_G(h)$. That is, $g \in \cap_{h \in G} C_G(h)$. On the other hand, if $g \in \cap_{h \in G} C_G(h)$, then $ghg^{-1} = h$ for all G, or equivalently $gh = hg$, showing $g \in Z(G)$. □

For parts (b) and (c), Lagrange's theorem (If H is a subgroup of G where $|G|$ is finite, then $|H|$ divides $|G|$) will be useful. To be specific, groups D_8 and Q_8 have order 8. If we know a *proper* subgroup has at least 4 elements, then it cannot have any more elements since 4 is the greatest divisor of 8 except for 8 itself.

(a) $S_3 = \{e, (12), (13), (23), (123), (132)\}$. First, let us consider $C_G(12) \supseteq \{e, (12)\}$. Then we compute $(13)^{-1}(12)(13) = (23)$, so $(13) \notin C_G(12)$. Likewise, we conclude that $(23) \notin C_G(12)$. You can either explicitly check that $(132)^{-1}(12)(132) = (23) \neq (12)$ or argue that if $(132) \in C_G(12)$, since $(132) = (12)(13)$ and $(12) \in C_G(12)$ and C_G is a group so $(13) \in C_G(12)$ which is a contradiction. We conclude $C_G(12) = \{e, (12)\}$.

From symmetry, we conclude $C_G(13) = \{e, (13)\}$ and $C_G(23) = \{e, (23)\}$.

Now we consider $C_G(132) \supseteq \{e, (132), (123)\}$ (since $(123) = (132)^2$). From above, we see that $(12)(132) \neq (132)(12)$, which also means $(12)(132)(12) \neq (132)$ (since $(12)^{-1} = (12)$). That is, $(12) \notin C_G(132)$. We can either argue by symmetry that $(23), (13) \notin C_G(132)$ or use Lagrange's theorem: $C_G(132)$ is a proper subgroup of S_3, so it can have at most three elements. In any case, we conclude that $C_G(132) = \{e, (132), (123)\}$.

Likewise, $C_G(123) = \{e, (132), (123)\}$.

Finally, we see from above claim that $Z(S^3) = \{e\}$.

(b) $D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Let us consider $C_G(r)$, which contains $\{e, r, r^2, r^3\}$. And we see that $s^{-1}rs = r^{-1} = r^3$ from the defining property of D_8, which shows $s \notin C_G(r)$. Hence $C_G(r)$ is a proper subgroup of D_8 which has at least 4 elements, but from Lagrange's theorem, we conclude $C_G(r) = \{e, r, r^2, r^3\}$.

Same is true for $C_G(r^3)$, as r and r^3 are located symmetrically in D_8. Likewise for $C_G(r)$, $C_G(r^3)$ contains $\{e, r, r^2, r^3\}$, but does not contain s, so $C_G(r^3) = \{e, r, r^2, r^3\}$.

On the other hand, while $C_G(r^2) \supseteq \{e, r, r^2, r^3\}$, $sr^2s = r^2$ so $s \in C_G(r^2)$ which shows $|C_G(r^2)| \geq 5$. From Lagrange's theorem, we conclude $C_G(r^2) = D_8$. Notice that this implies r^2 is in the center, or equivalently $r^2 \in C_G(g)$ for any $g \in D_8$.

Therefore, when we compute $C_G(s)$, we know that it contains $\{e, s, r^2\}$ from the beginning. Since $C_G(s)$ is a group, it also contains $s \cdot r^2 = sr^2$. But we know that $s^{-1}rs \neq r$ which is equivalent to $r^{-1}sr \neq s$, so again from Lagrange's theorem, $C_G(s) = \{e, s, r^2, r^2s\}$. We repeat this argument for elements sr, sr^2, sr^3 to conclude that $C_G(sr) = \{e, sr, r^2, sr^3\}$, $C_G(sr^2) = \{e, sr^2, s, r^2\}$ and $C_G(sr^3) = \{e, sr, sr^3, r^2\}$. Finally, $Z(D^8) = \{e, r^2\}$.

(c) $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Let us begin with the element -1. From one of the defining properties of the Quaternion group, we see that -1 commutes with all elements, or equivalently $C_G(-1) = Q_8$ or $-1 \in Z(Q_8)$ or $-1 \in C_G(g)$ for all $g \in Q_8$.

Now let us consider $C_G(i)$, which contains $\{1, i, -1, -i\}$. Then $ij = k \neq -k = ji$, which shows $jij^{-1} \neq i$ or $j \notin C_G(i)$. From Lagrange's theorem, we conclude that $C_G(i) = Q_8$. This argument applies to all other elements, showing that

$C_G(-i) = C_G(i)$,
$C_G(j) = C_G(-j) = \{1, j, -1, -j\}$,
$C_G(k) = C_G(-k) = \{1, k, -1, -k\}$,
and $Z(Q_8) = \{1, -1\}$.

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. Let $h \in H$. If we have $g \in H$ then it is trivial that $hgh^{-1} \in H$ (H subgroup) so $hHh^{-1} \subseteq H$. For the other inclusion, given any $g \in H$ we want to find $a \in H$ such that $g = hah^{-1}$. But $a = h^{-1}gh$ does this job. So $h \in N_G(H)$, showing $H \subseteq N_G(H)$. This automatically means $H \leq N_G(H)$, because if we pick two elements $a, b \in H$, $ab^{-1} \in H$ (subgroup criterion for $N_G(H)$).

For a counterexample, consider $G = S_3$ and $H = \{(12), (123)\}$. Then $(12)(123)(12) = (132)$, which shows that $(12)H(12) \neq H$, or $(12) \notin N_G(H)$.

(b). Show that $H \leq C_G(H)$ if and only if H is abelian. ($\Rightarrow$) Assume $H \leq C_G(H)$. For any $h \in H$ and for any $g \in H$, since $h \in C_G(H)$ we have $hgh^{-1} = g$ or $hg = gh$. H is abelian.

($\Leftarrow$) Assume H is abelian. Then for any $h \in H$, $hgh^{-1} = g$ whenever $g \in H$, showing that $h \in C_G(H)$. Therefore $H \subseteq C_G(H)$ and for the same reason as above, $H \leq C_G(H)$.

11. Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

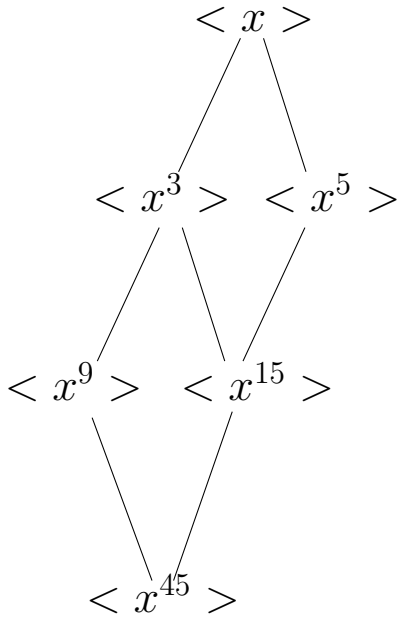
Let $z \in Z(G)$. Then $zg = gz$ for all $g \in G$. We want to show that $zAz^{-1} = A$ but all elements in zAz^{-1} has the form zaz^{-1} for some $a \in A$, while $zaz^{-1} = zz^{-1}a = a$ and hence $zAz^{-1} = A$. We get $Z(G) \subseteq N_G(A)$ and again, this directly implies $Z(G) \leq N_G(A)$.

Section 2.3

1. Find all subgroups of $Z_{45} =< x >$, giving a generator for each. Describe the containments.

We use Theorem 7. Since Z_{45} is finite, from part (3) of Theorem 7, we know that all subgroups of Z_{45} bijectively correspond with the positive divisors of 45, which are $1, 3, 5, 9, 15, 45$. We have subgroups $< x >= Z_{45}$, $< x^3 >$, $< x^5 >$,$< x^9 >$, $< x^{15} >$, and $< x^{45} >= \{0\}$. We claim that among these subgroups, $< x^j > \leq < x^i >$ if and only if i divides j. If i divides j, then $ik = j$ for some k and $(x^i)^k = x^j$ which means $x^j \in < x^i >$ and $< x^j > \leq < x^i >$. On the other hand, assume $< x^j > \leq < x^i >$ then in particular, $x^j \in < x^i >$ and hence $x^j = x^{ik}$ for some k. From Theorem 7 again, we have $\gcd(j, 45) = \gcd(ik, 45)$. Since j divides 45, we have $j = \gcd(ik, 45)$, which implies ik is a multiple of j. That is, i divides j.

From this claim, we get the following diagram:



2. Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

From Theorem 7, we deduce that an element $\overline{a} \in \mathbb{Z}/48\mathbb{Z}$ generates the whole group if and only if $\gcd(a, 48) = 1$. If gcd were not 1, then from part (3) of the theorem, $\overline{a}$ generates a subgroup which is equal to $< \gcd(a, 48) >$. If gcd were 1, $\overline{a}$ generates $< 1 >= \mathbb{Z}/48\mathbb{Z}$.

We simply collect positive integers less than 48 with $\gcd(a, 48) = 1$. The complete list is 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, and 47.

12. Prove that the following groups are not cyclic:

(a) $Z_2 \times Z_2$. This is a group of order 4, where every element has order 2. Therefore, it cannot be cyclic, since we need an element of order 4 (generator).

(b) $Z_2 \times \mathbb{Z}$. Assume it is cyclic, with generator (a, n). If $a = 0$, the element $(0, n)$ will never generate $(1, 0)$, as $(0, n)^k = (0, kn)$. So $a = 1$. If $n \neq \pm 1$, $(1, n)$ will not generate $(1, 1)$, since $(1, n)^k = (k \bmod 2, nk)$ but $nk \neq 1$ for any integer k if $n \neq \pm 1$. So our only choices are $(1, 1)$ and $(1, -1)$. However, they cannot generate $(0, 1)$, because for the first component to be zero, we need an even power of (1 ± 1), say $2k$, but then $(1, \pm 1)^{2k} = (0, \pm 2k)$ and $\pm 2k \neq 1$.

(c) $\mathbb{Z} \times \mathbb{Z}$. We proceed as above to show that our only options are $(1,1)$, $(1,-1)$, $(-1,1)$, and $(-1,-1)$. For instance, if we pick $(1,1)$, this element only generates elements of the form (n,n) for $n \in \mathbb{Z}$. But $(1,0) \in \mathbb{Z} \times \mathbb{Z}$ so this cannot be a generator. Likewise, no other options cannot generate $(1,0)$.

24. Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G < x >$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. Proof. By definition, $g \in N_G < x >$ means $g < x > g^{-1} =< x >$. In particular, $gxg^{-1} \in < x >$ so $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G < x >$. Proof. We want to show that $g < x > g^{-1} =< x >$. First, $gx^k g^{-1} = x^a$ implies $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$. This is a simple induction, since for $k = 1$ it is obvious and if we assume $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$ then $gx^{k+1}g^{-1} = gx^k xg^{-1} = gx^k g^{-1}(gxg^{-1}) = x^{ak}x^a = x^{(a+1)k}$. This shows $g < x > g^{-1} \leq < x >$. But from exercise 17 of Section 1.7, we know that $g < x > g^{-1}$ and $< x >$ have the same number of elements, so we have the equality.

26. Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \qquad \text{by} \qquad \sigma_a(x) = x^a$$

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. It should be clear that σ_a is a homomorphism.

Lemma. Let x generate Z_n. We first prove that $< \sigma_a(x) >= \sigma_a(Z_n)$. (The image of σ_a equals the subgroup of Z_n generated by $\sigma_a(x)$)

All elements in $\sigma_a(Z_n)$ are of the form $y^a = \sigma_a(y)$ for some $y \in Z_n$ but $y = x^b$ for some b. Hence $y^a = \sigma_a(x^b) = \{\sigma_a(x)\}^b$ and $< \sigma_a(x) > \supseteq \sigma_a(Z_n)$. On the other hand, if $y \in < \sigma_a(x) >$, $y = \{\sigma_a(x)\}^b = \sigma_a(x^b)$ so $y \in \sigma_a(Z_n)$.

Proof. For σ_a to be an automorphism, it should be surjective in particular, i.e.$\sigma_a(Z_n) = Z_n$. Since $\sigma_a(Z_n)$ is generated by $< \sigma_a(x) >=< x^a >$, from Theorem 7, this equals $< x >$ if and only if $\gcd(a,n) = 1$. And if it is surjective, it is automatically injective since domain and range has the same cardinality. Hence we are done.

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b (\mathrm{mod} n)$. Since σ_a is solely determined by $\sigma_a(x)$, $\sigma_a = \sigma_b$ if and only if $\sigma_a(x) = \sigma_b(x)$, or $x^a = x^b$. In a cyclic group of order n, $x^a = x^b$ if and only if $a - b \equiv 0 (\mathrm{mod} n)$, or $a \equiv b (\mathrm{mod} n)$.

(c) Prove that every automorphism of Z_n is equal to σ_a for some a. Let ϕ be an automorphism of Z_n. Then $\phi(x) = x^a$ for some a. Now we claim that $\phi = \sigma_a$. Any element of Z_n is of the form x^b for $b \in \mathbb{Z}$, and hence we compute $\phi(x^b) = \{\phi(x)\}^b = x^{ab}$ (from being a homomorphism), while $\sigma_a(x^b) = x^{ab}$. Hence they coincide on all elements of Z_n. This is essentially the proof that σ_a is solely determined by $\sigma_a(x)$.

(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. Proof of the first part: $\sigma_a \circ \sigma_b(x) = \sigma_a(x^b) = x^{ab} = \sigma_{ab}(x)$ and it implies directly that $\sigma_a \circ \sigma_b = \sigma_{ab}$ since they are both homomorphisms. Now let us show that this map is an isomorphism.

This map is *well-defined*, since whenever we have an element $a \in \mathbb{Z}/n\mathbb{Z}$ which is prime to n, σ_a is an automorphism of Z_n from part (a).

This map is a *homomorphism*, since $\sigma_a \circ \sigma_b = \sigma_{ab}$.

This map is *injective*, since if $\sigma_a = \sigma_b$, from part (b) we know $a - b \equiv 0 (\mathrm{mod} n)$, which means $a = b$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

This map is *surjective*, since every automorphism of Z_n is equal to σ_a for some a, (part (c)) and $\gcd(a, n) = 1$ from part (a).

Section 2.4

7. Prove that the subgroup of S_4 generated by (12) and $(13)(24)$ is isomorphic to the dihedral group of order 8.

Proof. Call this subgroup X. First compute that $(12) \cdot (13)(24) = (1324)$, and X is also generated by $a = (12)$ and $b = (1324)$. Now $(1324)(12)(1324) = (12)$. That is, the generators a, b of X satisfy the following relations:

$$\begin{cases} a^2 = 1 \\ b^4 = 1 \\ bab = a \end{cases}$$

which means we have a homomorphism $\phi : D_8 \to X$ defined by $\phi(r) = b$, $\phi(s) = a$. It is obvious that ϕ is surjective, but it is not clear that ϕ is injective since a, b might satisfy further relations. Maybe the best way to proceed is to exhibit that X has indeed 8 distinct elements. Then ϕ is injective as it was surjective and D_8 has 8 elements. Hence ϕ is an isomorphism.

Indeed, $X = \{(12), (13)(24), (1324), (1432), 1, (34), (12)(34), (14)(23)\}$. □

13. Prove that the multiplicative group of positive rational numbers is generated by the set

$$\{\frac{1}{p} \ : \ p \, \text{is a prime}\}$$

Proof. Any positive rational is expressed as $\frac{m}{n}$ where m, n are positive integers. We can write n and m as a product of primes, $n = p_1 p_2 ... p_k$ $m = q_1 q_2 ... q_l$ (where p_is and q_js are not necessarily distinct), then

$$\frac{1}{n} = \frac{1}{p_1} \times ... \times \frac{1}{p_k}$$

and

$$m^{-1} = \frac{1}{m} = \frac{1}{q_1} \times ... \times \frac{1}{q_l}$$

so $\frac{m}{n}$ is generated by rations of the form $\frac{1}{p}$. □

14. A group H is called finitely generated if there is a finite set A such that $H =< A >$.

(a) Prove that every finite group is finitely generated. This is trivial. Any group G is generated by all elements of the group, which is finite when G is finite.

(b) Prove that $\mathbb{Z}$ is finitely generated. We know 1 is a generator of $\mathbb{Z}$.

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.

Claim. For any two rationals a, b, there exists a rational number c such that the additive subgroup of $\mathbb{Q}$ generated by a, b equals the subgroup generated by c.

Proof. We can write $a = \frac{x}{y}$, $b = \frac{z}{w}$ where $\gcd(x, y) = \gcd(z, w) = 1$. Let $q = \gcd(y, w)$ and let us write $y = qy'$, $w = qw'$. We claim that $< \frac{x}{y'}, \frac{z}{w'} >=< \frac{\gcd(xw', zy')}{y'w'} >$. From the Euclidean Algorithm we have $k(xw') + t(zy') = \gcd(xw', zy')$ for some integers k, t.

Then

$$k \cdot \frac{x}{y'} + t \cdot \frac{z}{w'} = \frac{\gcd(xw', zy')}{y'w'} \in < \frac{x}{y'}, \frac{z}{w'} >,$$

so we get $< \frac{x}{y'}, \frac{z}{w'} > \supseteq < \frac{\gcd(xw', zy')}{y'w'} >$. On the other hand, for any integers m, n, $mxw' + nzy'$ is a multiple of $\gcd(xw', zy')$ (this is obvious), so we get the opposite containment. Now, it is easy to see that

$$< \frac{x}{y}, \frac{z}{w} >=< \frac{\gcd(xw', zy')}{qy'w'} > .$$

(basically, we divide everything in the group by q) □

Now let us prove the statement of the problem. Let X be a finitely generated group, and let $\{a_1, ..., a_k\}$ be a generating set for X such that k is minimal. If $k \neq 1$, then from above claim, we have $X =< a_1, ...a_{k-1}, a_k >=< a_1, ..., a_{k-2}, b >$ where $< a_{k-1}, a_k >=< b >$, contradicting the minimality of the generating set $\{a_1, ..., a_k\}$. Hence $k = 1$, or X is cyclic.

(d) Prove that $\mathbb{Q}$ is not finitely generated. From (c), It is enough to prove that $\mathbb{Q}$ is not cyclic. Any subgroup of a cyclic group is cyclic. Therefore, this will follow from exercise 15.

15. Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Consider the additive subgroup of $\mathbb{Q}$ generated by $\{1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, ...\}$. Any element of this subgroup is represented by $\frac{m}{2^k}$ for some k, m integers. We claim that this is not cyclic. If it were cyclic, let $\frac{m}{2^k}$ be the generator of this subgroup. However it cannot generate $\frac{1}{2^{k+1}}$. Contradiction.