Contents

2 Subgroups

2.1 Definition and Examples

Throughout these exercises, I will denote subgroups by H unless otherwise specified.

2.1.1

(a) Let $a+ai, b+bi \in H$. Then $a+ai-(b+bi) = (a-b)+(a-b)i \in H$

(b) Let $z, y \in H$. Then $|zy^{-1}| = |z||y^{-1}| = |z||y|^{-1} = 1 \cdot 1^{-1} = 1$, so $zy^{-1} \in H$

(c) Let $\frac{a}{b}, \frac{c}{d} \in H$. So $b, d | n$, so $xb = n, yd = n$ for ints x, y. Let $g = (b, d)$, and $l = (b, d)$.
(Recall from Chapter 0 that $gl = bd$, and also $g = rb + sd$ for some ints r, s).
Then $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} = \frac{\frac{1}{g}(ad-bc)}{\frac{1}{g}bd} = \frac{\frac{1}{g}(ad-bc)}{l}$. (Note that the numerator is an integer, since $g | ad-bc$).
We need to show that $l | n$.
Note that $m = \frac{gy}{b}$ is an integer, because

$$\begin{aligned}\frac{gy}{b} &= \frac{rby + sdy}{b} \\ &= ry + \frac{sdy}{b} \\ &= ry + \frac{sn}{b} \\ &= ry + sx\end{aligned}$$

and note that $l = \frac{bd}{g}$, so

$$\begin{aligned}lm &= \frac{bd}{g} \cdot \frac{gy}{b} \\ &= yd \\ &= n\end{aligned}$$

Hence $l | n$ as needed.

(d) Let $\frac{a}{b}, \frac{c}{d} \in H$, so $(b, n), (d, n) = 1$.
Suppose $(bd, n) > 1$, so there is an integer $s > 1$ such that $s | bd$ and $s | n$. Let p be a prime factor of s, so we have $p | n$ and $p | bd$. The latter implies that $p | b$ or $p | d$. Assume without loss of generality the former. Then $p | n$ and $p | d$, but $(b, n) = 1$, a contradiction. Hence $(bd, n) = 1$, and $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \in H$.

(e) Let $x, y \in H$. Then $x^2 = \frac{a}{b}, y^2 = \frac{c}{d}$, for $a, b, c, d \in \mathbb{Z}$. Then $(xy^{-1})^2 = x^2y^{-2} = \frac{ad}{bc}$. So $xy^{-1} \in H$.

2.1.2

We will show that closure is not satisfied in all these exercises

(a) $(3\ 1) \circ (1\ 2) = (1\ 2\ 3) \notin H$

(b) $r^{\lceil \frac{n}{2} \rceil}s$ is a reflection (across the line passing through the second vertex and origin), but $(r^{\lceil \frac{n}{2} \rceil}s)s = r^{\lceil \frac{n}{2} \rceil}$ which is a rotation

(c) Since n is composite, $n = ab$ for $0 < a, b < n$.
Let $x \in G$ with $|x| = n$. If H is a subgroup, note that x times itself a times must be in H by closure, i.e. $x^a \in H$. But $(x^a)^b = x^n = 1$, so $|x^a| \leq b < n$, so $x^a \notin H$ by definition, a contradiction.

(d) $1 + 1 = 2$

(e) Note that $\sqrt{2}, \sqrt{3} \in H$. But $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ which is irrational, so $\sqrt{2} + \sqrt{3} \notin H$.

2.1.3

(a) Each element is its own inverse, so we verify the operation is closed on the rest of the elements:

$$\begin{aligned}(r^2)(s) &= sr^{-2} = sr^2 \in H\\ (r^2)(sr^2) &= sr^{-2}r^2 = s \in H\\ (s)(r^2) &= sr^2 \in H\\ (s)(sr^2) &= s^2r^2 = r^2 \in H\\ (sr^2)(r^2) &= sr^4 = s \in H\\ (sr^2)(s) &= ssr^{-2} = s^2r^2 = r^2 \in H\end{aligned}$$

(b) Again, each element is its own inverse, so we verify closure:

$$\begin{aligned}(r^2)(sr) &= sr^{-2}r = sr^{-1} = sr^3 \in H\\ (r^2)(sr^3) &= sr^{-2}r^3 = sr \in H\\ (sr)(r^2) &= sr^3 \in H\\ (sr^3)(r^2) &= sr^5 = sr \in H\\ (sr^3)(sr) &= sr^3sr = s^2r^{-3}r = r^{-2} = r^2 \in H\end{aligned}$$

$(sr)(sr^3) = srsr^3 = s^2r^{-1}r^3 = s^2r^2 = r^2 \in H$

2.1.4

Let $G = \mathbb{Z}$, and H be the positive even integers.

2.1.5

Let $G = \{a_1, \ldots, a_2, \ldots, a_n = 1\}$ (the elements listed are distinct), and assume without loss of generality that $H = \{a_2, \ldots, a_n = 1\}$.
Note that we can't have $a_1a_2 = a_1$ or $a_1a_2 = a_2$, or else by cancelation we will have $a_2 = 1$ or $a_1 = 1$ respectively, both contradictions.
So assume without loss of generality that $a_1a_2 = a_3$ (it's okay if $n = 3$ and $a_3 = 1$), yielding

$$a_1 = a_3{a_2}^{-1} \tag{1}$$

- Case: ${a_2}^{-1} = a_1$.
  Then $a_2 \in H$, but ${a_2}^{-1} \notin H$, so inverses are not in H
- Case: ${a_2}^{-1} \neq a_1$
  Then ${a_2}^{-1} \in H$. But $a_3{a_2}^{-1} = a_1 \notin H$, so closure is not satisfied.

2.1.6

Let G be abelian and $g, h \in H$. Then $|g| = n, |h| = m$, with $n, m < \infty$.
Then $(gh^{-1})^{nm} = (g^n)^m(h^m)^{-n} = 1$. (The first equality follows from the fact that G is abelian). Hence, $|gh^{-1}| \leq nm \leq \infty$.
Now suppose $H = S_\infty$ a non-abelian group. Consider the permutations

$$\sigma = (1\ 2)(3\ 4)(5\ 6)\cdots \tau = (2\ 3)(4\ 5)(6\ 7)\cdots \tag{2}$$

Individually, they just swap elements, so $|\sigma|, |\tau| = 2$, but $|\tau \circ \sigma| = \infty$.

2.1.7

The torsion subgroup is clearly $H = 0 \times \mathbb{Z}/n\mathbb{Z}$
Let $I = (G - H) \cup \{0\}$
Then $(2,1), (2,0) \in I$. But $(2,1) - (2,0) = (0,1)$, is not in I (It is a nonzer element in H)

2.1.8

- Only if: Suppose $H \cup K$ is a subgroup
  Suppose $K \not\subset H$, so there exists $k \in K$ such that $k \notin H$
  Then let $h \in H$.
  Then $h, k \in H \cup K$, so $hk \in H \cup K$ (since $H \cup K$ is a subgroup).
  If $hk \in H$, then $h^{-1}(hk) \in H$, so $k \in H$, a contradiction.
  So we must have $hk \in K$. But then $(hk)k^{-1} \in K$, so $h \in K$.
  Since $h \in H$ was arbitrary, $H \subset K$
- If: Assume without loss of generality that $H \subset K$
  Let $x, y \in H \cup K$. Then $x, y \in K$ (since $H \subset K$), so $xy^{-1} \in K = H \cup K$

2.1.9

Let $A, B \in \mathrm{SL}_n F$, so $\det A, \det B = 1$. Then $\det AB^{-1} = \det A \det B^{-1} = 1$

2.1.10

(a) See next part

(b) Let $\{H_i\}_{i \in I}$ be a collection of subgroups of G and let $H = \bigcap_{i \in I} H_i$.
Then let $x, y \in H$. So for arbitrary i. $x \in H_i$ If $y \in H_i$ for all i, then $y^{-1} \in H_i$. Then $xy^{-1} \in H_i$. Since i was arbitrary $xy^{-1} \in H = \bigcap H_i$

2.1.11

(a) Let $(a,1), (k,1) \in H$. Then $(a,1)(k,1)^{-1} = (a,1)(k^{-1},1) = (ak^{-1},1) \in H$

(b) Analogous to above

(c) Let $(a,a), (b,b) \in H$. Then $(a,a)(b,b)^{-1} = (a,a)(b^{-1},b^{-1}) = (ab^{-1}, ab^{-1}) \in H$

2.1.12

(a) Let $x, y \in H$, with $x = a^n, y = b^n$. Then $xy^{-1} = a^n b^{-n} = (ab^{-1})^n \in H$ (note we used that A is abelian here)

(b) Let $x, y \in H$, so $x^n, y^n = 1$. Then $(xy^{-1})^n = x^n (y^n)^{-1} = 1$, so $xy^{-1} \in H$.

2.1.13

2.1.14

See (b). $r^{\lceil \frac{n}{2} \rceil} s$ is a reflection, but $(r^{\lceil \frac{n}{2} \rceil} s)s = r^{\lceil \frac{n}{2} \rceil}$ which does not have order 2 in general. For the case $n = 4$ consider the reflection sr across the line $y = 0$, and note that $s(sr) = r$ which has order 4

2.1.15

Let $H = \bigcup_{i=1}^{\infty} H_i$, and let $x, y \in H$. So $x \in H_i, y \in H_j$ for some i, j. Assume without loss of generality that $i \geq j$. Then $y \in H_i$, since $H_j \subset H_i$. So $xy^{-1} \in H_i \subset H$

2.1.16

The inverse of an upper triangular matrix is upper triangular (because the adjoint is upper triangular), and they are closed under multiplication

2.1.17

The same logic as above, with the additional note that diagonals of 1s are preserved after matrix multiplication. Diagonals of 1s are preserved by taking inverses too (the adjoint is the transpose of the cofactor matrix, and the minors along the diagonal are all clearly just 1)

2.2 Centralizers and Normalizers. Stabilizers and Kernels

2.2.1

Follows from

$$\begin{aligned} & gag^{-1} = a \\ \iff & ga = ag \\ & iff a = g^{-1}ag \end{aligned}$$

we will take these equivalences for granted moving forward

2.2.2

Let $x \in G$. And note that given $g \in Z(G)$, we have $gx = xg$. This is because by definition of $Z(G)$, x commutes with all elements of G, including g. But this also says that g commutes with all elements of x of $Z(G)$, so $g \in C_G(Z(G))$. Since $g \in G$ was arbitrary, $G \subset C_G(Z(G))$ and since the reverse inclusion trivially holds, $C_G(Z(G)) = G$.
We already know from the section that the centralizer is contained in the normalizer, i.e. $G = C_G(Z(G)) \subset N_G(Z(G))$, so again the trivial reverse inclusion yields $G = N_G(Z(G))$.

2.2.3

If $g \in C_G(B)$, then given $a \in A$, we have $a \in B$, so $ga = ag$ holds. Hence $g \in C_G(A)$ (since $a \in A$ was arbitrary). And since $g \in C_G(B)$ was arbitrary, $C_G(B) \leq C_G(A)$.

2.2.4

- S_3
  Recall that
  $$S_3 = \{1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \tag{3}$$
  of course $|S_3| = 6$, so all the centralizers must divide 6 (by Lagrange's theorem).
  Trivially, $C(1) = S_3$
  Now we note from the example in the text that, where $A = \{1, (1\ 2)\}$, $C_{S_3}(A) = A$. For now, denote $C = C(1, 2)$ for convenience
  By the previous exercises,

  $$\begin{aligned} & \{(1,2)\} \subset A \\ \implies & C(A) \leq C((1,2)) \\ \implies & |C(A)||C| \\ \implies & 2||C| \end{aligned}$$

  So we have $2||C||6$, which means we must have $|C| = 2$ or $|C| = 6$. But $(1\ 2)$ does not commute with $(1\ 2\ 3)$, so $|C| = 2$, and $C(A) \leq C$ implies that $C = C(A)$. I.e. we conclude that $C((1\ 2)) = \{1, (1\ 2)\}$. With entirely analogous arguments for the other "swapping" permutations, we obtain

  $$\begin{aligned} C((1\ 2)) &= \{1, (1\ 2)\} \\ C((1\ 3)) &= \{1, (1\ 3)\} \\ C((2\ 3)) &= \{1, (2\ 3)\} \end{aligned}$$

  Now denote $C = C((1\ 2\ 3))$. We have $1, (1\ 2\ 3) \in C$ automatically. And since C is a subgroup, we must have $(1\ 2\ 3)^{-1} = (1\ 3\ 2) \in C$. Now $|C| \leq 3$, but by $|C||6$, this narrows it down to $|C| = 3$ or $|C| = 6$. But since $(1\ 2)$

doesn't commute with (1 2 3), we must have $|C| = 3$. Hence, $C((1\ 2\ 3)) = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$. An analagous argument applies for $C((1\ 3\ 2))$, yielding the same set. So, in total, we have

$$\begin{aligned} C(1) &= S_3 \\ C((1\ 2)) &= \{1, (1\ 2)\} \\ C((1\ 3)) &= \{1, (1\ 3)\} \\ C((2\ 3)) &= \{1, (2\ 3)\} \\ C((1\ 2\ 3)) &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} \\ C((1\ 3\ 2)) &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} \end{aligned}$$

Finally, since all the centralizers are missing elements except for 1, we have $Z(S_3) = 1$

- D_8
  We have
  $$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \tag{4}$$
  So all centralizers must divide 8.
  The examples give us the following info. Where $A = \{1, r, r^2, r^3\}$,
  $$\begin{aligned} Z(D_8) &= \{1, r^2\} \\ C(A) &= A \end{aligned}$$
  So the center has already been computed, and of course $C(1) = D_8$.
  Next, we have
  $$\begin{aligned} &\{r\} \subset A \\ \implies &C(A) \leq C(r) \\ \implies &4 || C(r)| \end{aligned}$$
  Combined with the fact $|C(r)||8$, we must have $|C(r)| = 4$ or $|C(r)| = 8$. However, s and r don't commute ($rs = sr^{-1} \neq sr$), so $s \notin C(r)$ and we must hae $|C(r)| = 4$. Since $C(A) \leq C(r)$, this means that $C(r) = C(A)$. Analagously, $\{r^3\} \subset A$ implies $|C(r^3)| = 4$ or $|C(r^3)| = 8$, but s and r^3 don't commute, yielding $C(r^3) = C(A)$. Next, since $r^2 \in Z(D_8)$, we have $C(r^2) = D_8$. Thus, we have so far concluded that
  $$\begin{aligned} C(1) &= D_8 \\ C(r) &= \{1, r, r^2, r^3\} \\ C(r^2) &= D_8 \\ C(r^3) &= \{1, r, r^2, r^3\} \end{aligned}$$
  Now consider the element sr^k ($k = 0, 1, 2, 3$). Automatically, we have $1, r^2, sr^k \in C(sr^k)$. So $|C(sr^k)| \geq 3$. But $|C(sr^k)||8$, so we must have $|C(sr^k)| = 4$ or $|C(sr^k)| = 8$.
  Now note that
  $$\begin{aligned} (sr^k)r &= sr^{k+1} \\ r(sr^k) &= sr^{k-1} \end{aligned}$$
  Which are equal if and only if
  $$\begin{aligned} &sr^{k+1} = sr^{k-1} \\ \iff &r^k r = r^k r^{-1} \\ \iff &r = r^{-1} \end{aligned}$$
  which is impossible in D_8. Hence $r \notin C(sr^k)$, and we must conclude $|C(sr^k)| = 4$. Hence, we can conclude that
  $$C(sr^k) = \{1, r^2, sr^k, x_k\} \tag{5}$$

where x_k is another element in D_8 that commutes with sr^k.
We note that sr and sr^3 are inverses, and hence commute, so that covers the case $k = 1, 3$. Also, sr^2 commutes with s, covering the cases $k = 0, 2$. Hence, we can now list the centralizers for every element in D_8:

$$\begin{aligned} C(1) &= D_8 \\ C(r) &= \{1, r, r^2, r^3\} \\ C(r^2) &= D_8 \\ C(r^3) &= \{1, r, r^2, r^3\} \\ C(s) &= \{1, r^2, s, sr^2\} \\ C(sr) &= \{1, r^2, sr, sr^3\} \\ C(sr^2) &= \{1, r^2, s, sr^2\} \\ C(sr^3) &= \{1, r^2, sr, sr^3\} \end{aligned}$$

- Q_8
man suckmndick

2.2.5

(a) $G = S_3, A = \{\mathbf{1}, (1\ 2\ 3), (1\ 3\ 2)\}$.
In the previous exercise, we computed that $C((1\ 2\ 3)) = A$

$$\begin{aligned} &\{(1\ 2\ 3)\}A \\ \implies &C(A) \leq C((1\ 2\ 3)) \\ \implies &C(A) \leq A \\ \implies &|C(A)||3 \end{aligned}$$

- $C(A) = A$
So we must have $|C(A)| = 1$ or $|C(A)| = 3$. The latter corresponds to $C(A) = A$, since $C(A) \leq A$. And since $C(A) \leq A$, we're checking if the lements of A commute with each other. But each element in A commutes with 1 and each element in A commutes with itself. So all that's left to check is if $(1\ 2\ 3)$ and $(1\ 3\ 2)$ commute, which they do, since $(1\ 3\ 2) \in A = C((1\ 2\ 3))$. Hence $C(A) = A$.
- $N(A) = G$
Note that $A = C(A) \leq N(A)$, so $3||N(A)|$. since $|S_3| = 6$, we must have $N(A) = A$ or $N(A) = G$. But

$$\begin{aligned} (1\ 2)\mathbf{1}(1\ 2)^{-1} &= \mathbf{1} \\ &\in A \end{aligned}$$

and

$$\begin{aligned} (1\ 2)(1\ 2\ 3)(1\ 2)^{-1} &= (1\ 2)(1\ 2\ 3)(1\ 2) \\ &= (1\ 2)(1\ 3) \\ &= (1\ 3\ 2) \\ &\in A \end{aligned}$$

and

$$\begin{aligned} (1\ 2)(1\ 3\ 2)(1\ 2)^{-1} &= (1\ 2)(1\ 3\ 2)(1\ 2) \\ &= (1\ 2)(2\ 3) \\ &= (1\ 2\ 3) \\ &\in A \end{aligned}$$

Hence $(1\ 2) \in N(A)$, so $N(A) \neq A$ and we must have $N(A) = G$

(b) $G = D_8, A = \{1, s, r^2, sr^2\}$

- $C(A) = A$
  From the previous exercise, we know that $C(s) = A$. Then

$$\begin{aligned} & \{s\} \subset A \\ \implies & C(A) \leq C(s) \\ \implies & C(A) \leq A \\ \implies & |C(A)||4 \end{aligned}$$

  So we must have $|C(A)| = 1, 2$, or 4
  Now $1 \in C(A)$ trivially. And

$$\begin{aligned} sr^2 &= r^{-2}s = r^2 s \\ s(sr^2) &= s^2 r^2 = sr^{-2}s = (sr^2)s \end{aligned}$$

  so $s \in C(A)$. And $r^2(sr^2) = sr^{-2}r^2 = s = sr^4 = (sr^2)r^2$,
  so $r^2 \in C(A)$
  Hence, $|C(A)| \geq 3$, so we must have $|C(A)| = 4$, i.e. $C(A) = A$.
- $N(A) = G$
  We have that $C(A) \leq N(A) \leq D_8$, so $4||N(A)||8$, hence we must have $N(A) = A$ or $N(A) = D_8$
  But

$$\begin{aligned} rsr^{-1} &= sr^{-2} = sr^2 \in A \\ rr^r r^{-1} &= r^2 \in A \\ r(sr^2)r^{-1} &= rsr = s \in A \end{aligned}$$

  so $r \in N(A)$, and we must have $N(A) = G$

(c) $G = D_{10}, A = \{1, r, r^2, r^3, r^4\}$

- $C(A) = A$
  $C(A) \leq D_{10}$, so $|C(A)||10$. So we must have,
  $|C(A)| = 1, 2, 5$, or 10.
  The elements of A clearly commute with each other, so $A \leq C(A)$, leaving us with
  $|C(A)| = 5$ or 10
  But $rs = sr^{-1} \neq sr$, so $s \notin C(A)$ and we must have $|C(A)| = 5$, i.e. $C(A) = A$.
- $N(A) = G$
  As usual $C(A) \leq N(A) \leq D_{10}$, so
  $5||N(A)||10$,
  so we must have $|N(A)| = 5$ or 10
  Bute for $k = 0, \ldots, 4$, we have $sr^k s^{-1} = sr^k s = s^2 r^{-k} = r^{-k} = r^{5-k} \in A$
  so $s \in A$, which means we must have $|N(A)| = 10$, i.e. $N(A) = G$

2.2.6

(a) $H \leq N_G(H)$:
  If $h \in H$, then take arbitrary $g \in H$. Then $hgg^{-1} \in H$ (since H is a subgroup). Since g was arbitrary, $hHh^{-1} \subset H$, and the reverse inclusion is trivial (set $h = 1$, which we can do because H is a subgroup). Hence $hHh^{-1} = H$, and $h \in N(H)$. Since h was arbitrary, $H \subset N(H)$ i.e. $H \leq N(H)$
  For a counterexample when H is not a subgroups, let $G = S_3$ and $H = \{(1\ 2), (1\ 2\ 3)\}$. But $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) \notin H$. So $(1\ 2) \notin N(H)$

(b) $H \leq C_G(H)$ iff H abelian
  If H is abelian, let $h \in H$ and $g \in H$. Then g, h commute (since H abelian). Since $g \in H$ was arbitrary, $h \in C(H)$, and since $h \in H$ was arbitrary, $H \leq C(H)$
  If $H \leq C(H)$, let $h, g \in H$. Since $h \in H$ and $g \in C(H)$, g, h commute. Since $g, h \in H$ were arbitrary, H is abelian

2.2.7

We will do both parts in one
Suppose $r^i \in Z(D_{2n})$, $(i = 0, \ldots, n-1)$.
Suppose $r^i \in Z(D_{2n})$. Then

$$\begin{aligned} & sr^i = r^i s \\ \implies & sr^i = sr^{-i} \\ \implies & r^i = r^{-i} \\ \implies & r^{2i} = 1 \end{aligned}$$

This is only possible when $i = 0$ (the case $r^i = 1$), or when n is even and $i = n/2$
Suppose $sr^i \in Z(D_{2n})$, $(i = 0, \ldots, n-1)$. Then

$$\begin{aligned} & sr^i r = rsr^i \\ \implies & sr^{i+1} = sr^{i-1} \\ \implies & r^{i+1} = r^{i-1} \\ \implies & r = r^{-1} \end{aligned}$$

which never occurs for $n \geq 3$

2.2.8

The text already stated that the stabilizer is a subgroup
G_i can be easily identified with S_{n-1}, so $|G_i| = |S_{n-1}| = (n-1)!$

2.2.9

$N_H(A) \subset N_G(A)$ and $N_H(A) \subset H$ are trivial, so $N_H(A) \subset N_G(A) \cap H$.
Now let $h \in N_G(A) \cap H$. Then by definition of $N_G(A)$, $hAh^{-1} = A$, so $h \in N_H(A)$.

2.2.10

$|H| = 2$

- $N_G(H) = C_G(H)$:
  If $|H| = 2$, then $H = \{1, h\}$, for some $h \neq 1$ $(h = h^{-1})$.
  $C(H) \leq N(H)$ as always. So we prove the reverse inclusion. Let $g \in N(H)$. It trivially commutes with 1, so we have to show that it commutes with h as well.
  We do know that $ghg^{-1} \in H$ (since $g \in N(H)$). In the case $ghg^{-1} = 1$, we'd have $gh = g \implies h = 1$, a contradiction. So we must have $ghg^{-1} = h \implies gh = hg$ as needed.
- $N_G(H) = G \implies H \leq Z(G)$: If $N(H) = G$, then $C(H) = G$, as we have just shown. $C_G(H) = G$ means that the elements of H commute with all the elements of G. i.e. $H \subset Z(G)$.

2.2.11

Let $g \in Z(G)$. Then let $a \in A$. Then since g is in the center, $ga = ag \implies gag^{-1} = a \implies gag^{-1} \in A$. Since $a \in A$ was arbitrary, $gAg^{-1} \subset A$, and the reverse inclusion is trivial by $g = 1$, so $g \in N_G(A)$. Since $g \in G$ was arbitrary, $Z(G) \subset N_G(A)$

2.2.12

(a) We have

$$\begin{aligned} p &= 12x_1^5 x_2^7 x_4 - 18x_2^3 x_3 + 11x_1^6 x_2 x_3^3 x_4^{23} \\ \sigma &= (1\ 2\ 3\ 4) \\ \tau &= (1\ 2\ 3) \end{aligned}$$

And thus

$$\begin{aligned}
\sigma \cdot p &= 12x_2^5x_3^7x_1 - 18x_3^3x_4 + 11x_2^6x_3x_4^3x_1^{23} \\
\tau \cdot (\sigma \cdot p) &= 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23} \\
(\tau \circ \sigma) \cdot p &= \tau \cdot (\sigma \cdot p) && \text{(since this is an action, by the next part)} \\
(\sigma \circ \tau) \cdot p &= (1\ 3\ 2\ 4)p \\
&= 12x_3^5x_4^7x_1 - 18x_4^3x_2 + 11x_3^6x_4x_2^3x_1^{23}
\end{aligned}$$

(b) We verify the axioms

- Identity: $\mathbf{1} \cdot p(x_1, x_2, x_3, x_4) = p(x_{\mathbf{1}1}, x_{\mathbf{1}2}, x_{\mathbf{1}3}, x_{\mathbf{1}4}) = p(x_1, x_2, x_3, x_4)$ as needed
- Associativity: $\tau \cdot (\sigma \cdot p(x_1, x_2, x_3, x_4)) = \tau \cdot p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = p(x_{\tau(\sigma(1))}, x_{\tau(\sigma(2))}, x_{\tau(\sigma(3))}, x_{\tau(\sigma(4))}) = p(x_{\tau\circ\sigma(1)}, x_{\tau\circ\sigma(2)}, x_{\tau\circ\sigma(3)}, x_{\tau\circ\sigma(4)}) = (\tau \circ \sigma) \cdot p(x_1, x_2, x_3, x_4)$

(c) Stab, $x_4 = \{\mathbf{1}, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, which is clearly isomorphic to S_3

(d) Stab, $(x_1 + x_2) = \{\mathbf{1}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$

(e) Stab, $(x_1x_2 + x_3x_4) = \{\mathbf{1}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$. This is clearly isomorphic to D_8, if you label the vertices clockwise as $1, 3, 2, 4$.

(f) Trivial

2.2.13

Identical proof to (b)

2.2.14

Let $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and suppose $A \in Z(H(F))$ Then given $B = \begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$, we must have

$$\begin{gathered}
AB = BA \\
\implies \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}
\end{gathered}$$

which yields the equation

$$\begin{gathered}
f + ag + b = b + ce + f \\
\implies ag = ce
\end{gathered}$$

Setting $g, e = 1$ gives $a = c$. And setting $g = 1, e = 0$ gives $a = 0$, so also $c = 0$
Hence

$$Z(H(F)) = \{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} | b \in F \} \tag{6}$$

which can clearly be identified with F

2.3 Cyclic Groups and Cyclic Subgroups

2.3.1

2.3.2

2.3.3

2.3.4

2.3.5

2.3.6

2.3.7

2.3.8

2.3.9

2.3.10

2.3.11

2.3.12

(a) $Z_2 \times Z_2 = \{(0,0),(0,1),(1,0),(1,1)\}$, And all cyclic subgroups take the form $< x >= \{(0,0), x\}$, so $| < x > | < |Z_2 \times Z_2|$ in all cases.

(b) Given $a, b \in \mathbb{Z}$

$$(1,0) \notin < (0,a) >$$
$$(0,1) \notin < (1,b) >$$

So no cyclic subgroup generates all of $Z_2 \times \mathbb{Z}$

(c) The cyclic subgroups $< (0,y) >, < (x,0) >$ are always 0 in one coordinate and hence do not generate $\mathbb{Z} \times \mathbb{Z}$. The cyclic subgroup $< (x,y) >$ comprises only the line through the origin with a slope of y/x, not the entire $\mathbb{Z} \times \mathbb{Z}$ plane.

2.3.13

(a) $\mathbb{Z}$ is cyclic but $\mathbb{Z} \times Z_2$ is not

(b) Consider a homomorphism $\mathbb{Q} \to \mathbb{Q} \times Z_2$. If $a \mapsto (x,0)$, then there is no way to reach $(0,1)$. If $a \mapsto (y,1)$, there is no way to reach $(1,0)$.

2.3.14

2.3.15

If $\mathbb{Q} \times \mathbb{Q}$ was cyclic, then we'd have an isomorphism $\mathbb{Z} \to \mathbb{Q} \times \mathbb{Q}$. But if $1 \mapsto (b,c)$, that determines the rest of the map as $k \mapsto (kb, kc)$, which is obviously not surjective.

2.3.16

- Let $l = \text{lcm}, (m,n)$ and write $l = am = bn$. Then

$$\begin{aligned} (xy)^l &= x^l y^l && (x, y \text{ commute}) \\ &= (x^n)^b (y^m)^a \\ &= 1 \cdot 1 \\ &= 1 \end{aligned}$$

Hence by proposition 3 in the text, $|xy||l$

- If x, y do not commute, see my 2.1.6 for a counterexample
- Note that in D_{12}, $|r^2| = 3, |s| = 2$, so the lcm of the orders is 6. But $(sr^2)^2 = sr^2sr^2 = ssr^{-2}r^2 = s^2r^0 = 1 \cdot 1 = 1$, so $|sr^2| = 2 < 6$

2.3.17

$Z_n =< x|x^n = 1 >$

2.3.18

Let $\phi : Z_n \to H$ with $x \mapsto h$. Then if ϕ is a homomorphism, we must have $x^k \mapsto h^k$, uniquely determining ϕ if it exists.
If $x^a = x^b$, then $x^{a-b} = 1$, so $a - b = cn$ for some c. Then $\phi(x^a) = h^a$ and $\phi(x^b) = h^b$. But

$$\begin{aligned} & h^{a-b} = (h^n)^c \\ \implies & h^{a-b} = 1 \\ \implies & h^a = h^b \\ \implies & \phi(x^a) = \phi(x^b) \end{aligned}$$

So ϕ is well-defined and thus exists.

2.3.19

Let $\phi : \mathbb{Z} \to H$ with $1 \mapsto h$. Then if ϕ is a homomorphism we must have $\phi(k) = k\phi(1) = h^k$, uniquely determining ϕ.

2.3.20

Suppose $x^{p^n} = 1$. Let $o = |x|$. We know from prop 3 that $o|p^n$, so $ao = p^n$ for some $a \in \mathbb{Z}$ (assume wlg a positive). But the prime factorization is unique, so ao must factor into p^n, Hence $o = p^m$ for some $m \leq n$

2.3.21

2.3.22

2.3.23

2.3.24

(a) Trivial

(b) The proof is traced out. $gx^kg^{-1} = (gxg^{-1})^k = (x^a)^k = x^k \in < x >$, so $g < x > g^{-1} \leq < x >$ indeed. Now let $n = |x|$. Given $0 \leq i \leq k \leq n - 1$, suppose $gx^kg^{-1} = gx^ig^{-1}$. Then by right multiplying by g and left multiplying by g^{-1} on both sides,

$$\begin{aligned} & x^k = x^i \\ \implies & x^{k-i} = 1 \\ \implies & k - i = 0 && \text{(since } 0 \leq i \leq k \leq n - 1\text{)} \\ \implies & k = i \end{aligned}$$

The contrapositive yields that the gx^kg^{-1} are distinct for $k = 0, \ldots, n-1$. Hence $|g < x > g^{-1}| = n = | < x > |$, so $|g < x > g^{-1}| =< x >$.

2.3.25

- Let $|G| = n$ and $G =< x >$
  We have $(k, n) = 1$. Select i, j such that $0 \leq i \leq j \leq n-1$, and suppose $(x^i)^k = (x^j)^k$. Then

$$\begin{aligned}
& x^{ik} = x^{jk} \\
\implies & x^{jk-ik} = 1 \\
\implies & x^{k(j-i)} = 1 \\
\implies & n | k(j-i) && \text{(since } |x| = n\text{)} \\
\implies & n | j-i && \text{(since } (k,n) = 1\text{)} \\
\implies & j - i = 0 && \text{(since } 0 \leq i \leq j \leq n-1\text{)} \\
\implies & j = i
\end{aligned}$$

  Hence the powers by the residues are all distinct, so the image has order n and hence comprises all of G, so the map is surjective.

- We prove the following lemma:

  Lemma 2.1. *Let $|G| = n < \infty$, $(k, n) = 1$. Then $x^k = 1 \implies x = 1$ (so nonidentity elements taken to the kth power are never the identity)*

  Proof. Let $m = |x^k|$. Note that $|x^k| = | < x^k > |$, and hence by Lagrange's theorem, $m|n$. Suppose $m = 1$. Then $|x^k| = 1$ so $x^k = 1$, and $|x||k$. But $|x| = | < x > ||n$ by Lagrange's theorem, so $(k, n) \geq |x|$. But $(k, n) = 1$, so $|x| = 1$, i.e. $x = 1$ □

  $1^k = 1$, of course. Now take $x \in G, x \neq 1$. Then by the lemma, $x^k = y$ for some $y \neq 1$. Now suppose we also have $z \in G$ with $z^k = y$. Denote $zx^{-1} = a$. Then

$$\begin{aligned}
& z^k = y \\
\implies & z^k = x^k \\
\implies & z^k (x^{-1})^k = 1 \\
\implies & a^k = 1
\end{aligned}$$

  By the lemma, we would have $a = 1$, so $zx^{-1} = 1$ i.e. $z = x$. Hence the map is injective, and an injective map to itself must be surjective.

2.3.26

Let $Z_n =< x >$

(a) As shown in the first part of the previous exercise **??**, σ_a is injective and surjective.

(b)

$$\begin{aligned}
& \sigma_a = \sigma_b \\
\iff & \sigma_a(x) = \sigma_b(x) && \text{(The value on } x \text{ determines the whole map)} \\
\iff & x^a = x^b \\
\iff & x^{a-b} = 1 \\
\iff & n | a - b \\
\iff & a \equiv b \pmod{n}
\end{aligned}$$

(c) Let $\sigma \in \text{Aut}, (Z_n)$. Then $\sigma(x) = x^a$ for some $a \in \mathbb{Z}$
If σ is an automorphism, then

$$x^0, x^a, x^{2a}, \ldots, x^{(n-1)a} \tag{7}$$

are all distinct. Suppose $(a, n) = k$. Write $a = kb, n = km$. Note that $0 < m \leq n$. Then

$$x^{am} = x^{kbm} = x^{kmb} = x^{nb} = 1 \tag{8}$$

In order to not contradict the distinctness of the 7, we must have $m = n$. But then $n = km \implies k = 1$. I.e. $(a, n) = 1$, as needed.

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