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) $r^{\lfloor \frac{n}{2} \rfloor}s$ is a reflection, but $(r^{\lfloor \frac{n}{2} \rfloor}s)s = r^{\lfloor \frac{n}{2} \rfloor}s \notin H$

(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:

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

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

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)