Chapter 1

Groups

1.1 Semigroups, monoids and groups

Exercise 1.1.1. Give examples other than those in the text of semigroups and monoids that are not groups.

Answer. Semigroup: $(\mathbf{Z}_+, +)$
Monoid: $(\mathbf{Z}_+, \times)$

Exercise 1.1.2. Let G be a group (written additively), S a nonempty set, and $M(S, G)$ the set of all functions $f : S \to G$. Define addition in $M(S, G)$ as follows: $(f + g) : S \to G$ is given by $s \to f(s) + g(s) \in G$. Prove that $M(S, G)$ is a group, which is abelian if G is.

Answer. Firstly we check $M(S, G)$ is a group

1. $f + g : s \to f(s) + g(s) \in G$, so $f + g \in M(S, G)$
2. $(f + g) + h : s \to (f(s) + g(s)) + h(s)$, G is a group, so $s \to (f(s) + g(s)) + h(s) \Leftrightarrow s \to f(s) + (g(s) + h(s))$, $(f + g) + h = f + (g + h)$.
3. Take the unit element as $e' : s \to e$. $f + e' : s \to f(s) + e'(s) = f(s) + e = f(s)$, so $f + e' = f$. Similarly, $e' + f = f$.
4. For any $f \in M(S, G)$, take $f^{-1} : s \to (f(s))^{-1}$, whence $f(s) + (f(s))^{-1} = (f(s))^{-1} + f(s) = e$.

In conclusion, $M(S, G)$ is a group. If G is abelian $f + g : s \to f(s) + g(s) = g(s) + f(s)$, $f + g = g + f$, so $M(S, G)$ is abelian.

Exercise 1.1.3. Is it true that a semigroup which has a left identity element and in which every element has a right inverse (see Proposition 1.3) is a group?

Answer. If e is the left identity, $\forall a \in A, ea = a$ and $\forall a \in A, \exists a^{-1} s.t. aa^{-1} = e$. We have proved that if $cc = c$, then $c = e$.

$$(a^{-1}a)(a^{-1}a) = a^{-1}(aa^{-1})a = a^{-1}(ea) = a^{-1}a \Rightarrow a^{-1}a = e$$

a^{-1} is also the left inverse. $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$, e is also the right identity.

Exercise 1.1.4. Write out a multiplication table for the group D_4^*.

Answer. $D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{13}, T_{24}\}$

	I	R	R^2	R^3	T_x	T_y	T_{13}	T_{24}
I	I	R	R^2	R^3	T_x	T_y	T_{13}	T_{24}
R	R	R^2	R^3	I	T_{13}	T_{24}	T_y	T_x
R^2	R^2	R^3	I	R	T_y	T_x	T_{24}	T_{13}
R^3	R^3	I	R	R^2	T_{24}	T_{13}	T_x	T_y
T_x	T_x	T_{24}	T_y	T_{13}	I	R^2	R^3	R
T_y	T_y	T_{13}	T_x	T_{24}	R^2	I	R	R^3
T_{13}	T_{13}	T_y	T_{24}	T_x	R^3	R	I	R^2
T_{24}	T_{24}	T_x	T_{13}	T_y	R	R^3	R^2	I

Exercise 1.1.5. Prove that the symmetric group on n letters, S_n, has ordrer $n!$.

Answer. For a set A whose order is n, we prove there's $n!$ different bijections by induction

1. For $n = 1$, trivial.
2. Assume $n = k$, there's $k!$ bijections. For $n = k + 1$m fix one element in A, and take $a \to a$, there's k free elements, so there's $K! \cdot (k + 1)$ bijections in total.

By induction, we get the result.

Exercise 1.1.6. Write out an addition table for $Z_2 \oplus Z_2$. $Z_2 \oplus Z_2$ is called the Klein four group.

Answer. $Z_2 = \{1, 0\}$, $Z_2 \oplus Z_2 = \{(1, 1), (1, 0), (0, 1), (0, 0)\}$

	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Exercise 1.1.7. If p is prime, then the nonzero elements of Z_p form a group of order $p-1$ under multiplication. Show that this statement is false if p is not prime.

Answer. For the set $Z_p \backslash \{\bar{0}\}$

1. $Z_p \backslash \{\bar{0}\}$ is obviously associative and communicative.
2. Take $\bar{1}$ as the identity element, $\forall \bar{a} \in Z_p \backslash \{\bar{0}\}, \bar{1} \times \bar{a} = \bar{a}$.
3. We prove there is a unique element $a^{-1} \in Z_p \backslash \{\bar{0}\} s.t. aa^{-1} = \bar{1}$. Assume there exists $\bar{b}, \bar{c}$ and $\bar{a} \cdot \bar{b} = \bar{k}, \bar{a} \cdot \bar{c} = \bar{k}$, then $a(b-c) \equiv 0 \mod p$. p is a prime, so $lcm(p,a) = 1, lcm(p, b-c) = 1$, so $\bar{b} = \bar{c}$. There is at most one element s.t. $\bar{a}\bar{b} = \bar{k}$. Take $\bar{b} = \bar{1}, \bar{2}, \ldots p \bar{-} 1$, $\bar{k}$ travels through $\bar{b} = \bar{1}, \bar{2}, \ldots p \bar{-} 1$. There exists an element $\bar{b} \in Z_p \backslash \{\bar{0}\}, \bar{a}\bar{b} = \bar{1}$.

$Z_p \backslash \{\bar{0}\}$ is a group. If p is not a prime, the inverse element is not always unique. Take $a|p$, there's more than one inverse element in $Z_p \backslash \{\bar{0}\}$.

Exercise 1.1.8.

1. The relation given by $a\ b \Leftrightarrow a-b \in \mathbf{Z}$ is a congruence relation on the additive group $\mathbf{Q}$ [see Theorem 1.5].
2. The set $\mathbf{Q}/\mathbf{Z}$ of equivalence classes is an infinite abelian group.

Answer.

1. For group $(\mathbf{Q}, +)$, $a_1\ b_1 \Leftrightarrow a_1 - b_1 = k_1 \in \mathbf{Z}$, $a_2\ b_2 \Leftrightarrow a_2 - b_2 = k_2 \in \mathbf{Z}$, so $(a_1+a_2)-(b_1+b_2) = ((k_1+b_1)+(k_2+b_2))-(b_1+b_2) = k_1 + k_2 \in \mathbf{Z}$. $a\ b$ is a congruence relation.
2. 1 if $a+b \geq 1$, $\bar{a} + \bar{b} = a + \bar{b} - 1$. If $a+b < 1$, $\bar{a} + \bar{b} = a \bar{+} b$.
   2 $\mathbf{Q}/\mathbf{Z}$ is obviously associative and communicative.
   3 Take the identity element as $\bar{0}$, $\bar{0} + \bar{a} = \bar{a}$.
   4 If $\bar{a} \neq 0$, take $(\bar{a})^{-1} = 1 \bar{-} a$, then $\bar{a} + 1 \bar{-} a = \bar{0}$
   so $\mathbf{Q}/\mathbf{Z}$ is a abelian group. (Infinite remains to be certified)

Exercise 1.1.9. Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of $p(p^i, i > 0)$. Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.

Answer. Trivial.

Exercise 1.1.10. Let p be a prime and let $Z(p^\infty)$ be the following subset of the group $\mathbf{Q}/\mathbf{Z}$:

$$Z(p^\infty) = \{\overline{a/b} \in \mathbf{Q}/\mathbf{Z} | a, b \in \mathbf{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}$$

Show that $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbf{Q}/\mathbf{Z}$.

Answer. $Z(p^\infty) = \{\overline{a/b} | a, b \in \mathbf{Z}, b = p^i, i \geq 0\}$. Take $a = \frac{\bar{a_1}}{b_1}$, $b = \frac{\bar{a_2}}{b_2}$. $b^{-1} = \frac{\overline{b_2 - a_2}}{b_2}$

$$\begin{aligned} a + b^{-1} &= \frac{\bar{a_1}}{b_1} + \frac{\overline{b_2 - a_2}}{b_2} = \frac{\bar{a_1}}{p^{s_1}} + \frac{\overline{p^{s_2} - a_2}}{p^{s_2}} \\ &= \frac{\overline{a_1 \cdot p^{s_2} + p^{s_1}(p^{s_2} - a_2)}}{p^{s_1+s_2}} \in Z(p^\infty) \end{aligned}$$

Therefore, $Z(p^\infty)$ is a subgroup of $\mathbf{Q}/\mathbf{Z}$. $\frac{1}{p^i} \in Z(p^\infty)$ for any $i \in \mathbf{Z}$, so $Z(p^\infty)$ is infinite, $\mathbf{Q}/\mathbf{Z}$ is also infinite.

Exercise 1.1.11. The following conditions on a group G are equivalent:

- i G is abelian;
- ii $(ab)^2 = a^2b^2$ for all $a, b \in G$;
- iii $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$;
- iv $(ab)^n = a^nb^n$ for all $n \in \mathbf{Z}$ and all $a, b \in G$;
- v $(ab)^n = a^nb^n$ for three consecutive integers n and all $a, b \in G$. Show that v$\Rightarrow$ i is false if 'three' is replaced by 'two'.

Answer. i$\Leftrightarrow$ iii: $((ab)b^{-1})a^{-1} = (ab)(b^{-1}a^{-1}) = e$, so $(ab)^{-1} = b^{-1}a^{-1}$. If iii, $b^{-1}a^{-1} = a^{-1}b^{-1}$ for any $a, b \in G$, G is abelian. If i, G is abelian, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.
iv $\Rightarrow$ v, iv$\Rightarrow$ ii and i$\Rightarrow$ iv are trivial.
ii$\Rightarrow$ i:

$$(ab)(ab) = aabb \Rightarrow a^{-1}(ab)^2b^{-1} = a^{-1}aabbb^{-1} = ba = ab$$

so G is abelian.

v $\Rightarrow$ i: $a^n b^n = (ab)^n$, $a^{n-1}b^{n-1} = (ab)^{n-1}$, $a^{n+1}b^{n+1} = (ab)^{n+1}$.

$$(b^{-1})^n(a^{-1})^n = ((ab)^n)^{-1} = ((ab)^{-1})^n$$

$$((ab)^{-1})^n(ab)^{n+1} = (b^{-1})^n ab^{n+1}$$

$$((ab)^{-1})^n(ab)^{n-1} = b^{-1}a^{-1} = (b^{-1})^n a^{-1}b^{n-1}$$

$$a = (b^{-1})^n ab^n \qquad b^{-1}a^{-1}b = (b^{-1})^n a^{-1}b^n$$

So $a^{-1} = b^{-1}a^{-1}b$, which means G is abelian.
If "three" is replaced by "two": $a^n b^n = (ab)^n$, $a^{n+1}b^{n+1} = (ab)^{n+1}$.

$$(b^{-1})^n(a^{-1})^n = ((ab)^{-1})^n \qquad a = (b^{-1})^n ab^n$$

For the group $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, taking any $a \in S_3$, we can check that $a^6 = (1)$. If $n = 6$, then $a = (b^{-1})^n ab^n$ for any $a, b \in S_3$. But S_3 is nonabelian.

Exercise 1.1.12. If G is a group, $a, b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbf{N}$, then $b^j ab^{-j} = a^{r^j}$ for all $j \in \mathbf{N}$.

Answer. $bab^{-1} = a^r$. We prove it by induction. For $j = 1$, its always true. Assume $j = k$ the equation is correct, $b^k ab^{-k} = a^{r^k}$. $ba^{r^k}b^{-1} = (a^{r^k})^{r = a^{r^{k+1}}}$. For $j = k+1$, it's also true.

Exercise 1.1.13. If $a^2 = e$ for all elements a of a group G, then G is abelian.

Answer.

$$a^2 = e \Rightarrow a^2a^{-1} = ea^{-1} = a(aa^{-1}) = ae \Rightarrow a = a^{-1}$$

$$ab = a^{-1}b^{-1} = (ab)^{-1} = (ba)^{-1}$$

So $ab = ba \forall a, b \in G$. G is abelian.

Exercise 1.1.14. If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

Answer. Suppose not. $\forall a \neq e, aa \neq e \Leftrightarrow a \neq a^{-1}$. We can classify the group into some subsets. $G = \bigcup_{a \neq e} \{a, a^{-1}\} \cup \{e\}$. Notice that $\{a, a^{-1}\} \cap \{b, b^{-1}\} = \oslash$ if $a \neq b$, so $|G| = 2n + 1$, That's contradictory!

Exercise 1.1.15. Let G be a nonempty finite set with an associative binary operation such that for all $a, b, c \in G$, $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Then G is a group. Show that this conclusion may be false if G is finite.

Answer. G is a semigroup. Fix $a \in G$ and take b travels through all elements in G, then ab travels through all elements in G.
There exists an element e_1 s.t. $ae_1 = a \forall a \in G$. Similarly, we can find e_2 s.t. $e_2 a = a \forall a \in G$. $e_2 e_1 = e_1 = e_2 = e$. e is the identity element of G. Easily, we can find that $\forall a \in G, \exists! a^{-1} \in G$ s.t. $a^{-1}a = aa^{-1} = e$ because $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.
G is a group. If G is infinite, G may not be a group, for example: $(Z_+, \times)$.

Exercise 1.1.16. Let $a_1, a_2, \ldots$ be a sequence of elements in a semigroup G. Then there exists a unique function $\Psi : \mathbf{N}^* \to G$ such that $\Psi(1) = a_1, \Psi(2) = a_1 a_2, \Psi(3) = (a_1 a_2) a_3$ and for $n \geq 1$, $\Psi(n+1) = (\Psi(n)) a_{n+1}$. Note that $\Psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$.

Answer. Applying the Recursion Theorem with $a = a_1, S = G$ and $f_n : G \to G$ given by $x \to x a_{n+2}$ yields a function $\phi : \mathbf{N} \to G$. Let $\Psi = \phi\theta$, where $\theta : \mathbf{N}^* \to \mathbf{N}$ is given by $k \to k - 1$.

1.2 Homomorphisms and subgroups

Exercise 1.2.1. If $f : G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are not groups.

Exercise 1.2.2. A group G is abelian if and only if the map $G \to G$ given by $x \to x^{-1}$ is automorphism.

Exercise 1.2.3. Let Q_8 be the group(under ordinary matrix multiplication) generated by complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a nonabelian group of order 8. Q_8 is called the quaternion group.

Exercise 1.2.4. Let H be the group(under ordinary matrix multiplication) of real matrices generated by $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that H is a nonabelian group of order 8 which is not isomorphic to the quaternion group, but is isomorphic to the group D_4^*.

Exercise 1.2.5. Let S be a nonempty subset of a group G and define a relation on G by a b if and only if $ab^{-1} \in S$. Show that is an equivalence relation if and only if S is a subgroup of G.

Exercise 1.2.6. A nonempty finte subset of a group is s subgroup if and only if it is closed under the product in G.

Exercise 1.2.7. If n is a fixed integer, then $\{kn|n \in \mathbf{Z}\} \subset \mathbf{Z}$ is an additive subgroup of $\mathbf{Z}$, which is isomorphic to $\mathbf{Z}$.

Exercise 1.2.8. The set $\{\sigma \in S_n|\sigma(n) = n\}$ is a subgroup of S_n which is isomorphic to S_{n-1}.

Exercise 1.2.9. Let $f : G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H.

1. Ker$f$ and $f^{-1}(B)$ are subgroups of G.
2. $f(A)$ is a subgroup of H.

Exercise 1.2.10. List all subgroups of $Z_2 \oplus Z_2$. Is $Z_2 \oplus Z_2$ isomorphic to Z_4?

Exercise 1.2.11. If G is a subgroup, then $C = \{a \in G|ax = xa \text{ for all } x \in G\}$ is a abelian subgroup of G. C is called the center of G.

Exercise 1.2.12. The group D_4^* is not cyclic, but can be generated by two elements. The same is true of S_n(nontrivial). What is the minimal number of generators of the additive group $\mathbf{Z} \oplus \mathbf{Z}$?

Exercise 1.2.13. If $G = \langle a \rangle$ is a cyclic group and H is any group, then every homomorphism $f : G \to H$ is completely determined by the element $f(a) \in H$.

Exercise 1.2.14. The following cyclic subgroups are all isomorphic: the multiplication group $\langle i \rangle$ in $\mathbf{C}$, the additive group $\mathbf{Z_4}$ and the subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ of S_4.

Exercise 1.2.15. Let G be a group and Aut$G$ is the set of all automorphisms of G.

1. Aut$G$ is a group with composition of functions as binary operation.
2. Aut$\mathbf{Z} \cong Z_2$ and Aut$Z_6 \cong Z_2$; Aut$Z_8 \cong Z_2 \oplus Z_2$; Aut$Z_p \cong Z_{p-1}$ (p prime).
3. What is $\mathrm{AutZ_n}$ for arbitrary $n \in \mathbf{N}^*$?

Exercise 1.2.16. For each prime p the additive subgroup $Z(p^\infty)$ of $\mathbf{Q}/\mathbf{Z}$ is generated by the set $\{1/\bar{p}^n | n \in \mathbf{N}^*\}$.

Exercise 1.2.17. Let G be an abelian group and let H, K be subgroups of G. Show that the join $H \vee K$ is the set $\{ab | a \in H, b \in K\}$. Extend this result to any finite number of subgroups of G.

Exercise 1.2.18.

1. Let G be a group and $\{H_i | i \in I\}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i \in I} H_i$ is a subgroup, that is $\bigcup_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$.
2. Given an example of a group G and a family of subgroups $\{H_i | i \in I\}$ such that $\bigcup_{i \in I} H_i \neq \left\langle \bigcup_{i \in I} H_i \right\rangle$.

Exercise 1.2.19.

1. The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice in which the g.l.b of $\{H_i | i \in I\}$ is $\bigcap_{i \in I} H_i$ and the l.u.b is $\left\langle \bigcap_{i \in I} H_i \right\rangle$.
2. Exhibit the lattice of subgroups of the groups S_3, D_4^*, Z_6, Z_{27} and Z_{36}.