1 Groups
1.1 Semigroups,monoids and groups

1. If $n = 3$, then $|A_n| = \frac{1}{3}C_4^3 = 2$. In this case, there are only two ways of placing brackets. $(a_1a_2)a_3 = a_1(a_2a_3)$, hence this formula is true for $n = 3$. Assume that the formula is true for $n < k$. Let $n = k$, consider last two brackets, since divides $a_1...a_n$ into two parts, then we do not need to place brackets any more. Assume that the first one between two parts contains t elements, and the other contains $k - t$ elements, then there are $|A_t| \cdot |A_{k-t}|$ ways to place brackets in this case, hence

$$|A_k| = \sum_{i=1}^{k-1} |A_i||A_{k-i}| = \sum_{i=1}^{k-1} (\frac{1}{i}C_{2i-2}^{i-1})(\frac{1}{k-i}C_{2k-2i-2}^{k-i-1}) = \frac{1}{k}C_{2k-2}^{k-1}.$$

2. Define $a_1a_2...a_n := \prod_{i=1}^n a_i$ inductively for $a_1, ..., a_n \in S$, i.e.,

$$\prod_{i=1}^{n+1} a_i = (\prod_{i=1}^{n}) \cdot a_{n+1}.$$

We will prove this claim by induction on n. If $n = 3$, then

$$\prod_{i=1}^{3} a_i = (a_1a_2)a_3.$$

And the another way of placing bracket is $a_1(a_2a_3)$, according to the associative of S, then $\prod_{i=1}^3 a_i = a_1(a_2a_3)$. Hence the claim is true for $n = 3$.Assume that the claim is true for $n < k$. Let $n = k > 3$, any ways of placing bracket can divide $a_1a_2...a_n$ into two parts, if the first one between two parts contains t elements, and the other contains $k - t$ elements, i.e.

$$(a_1a_2...a_t)(a_{t+1}a_{t+2}...a_k) = \prod_{i=1}^{t} a_i \prod_{j=t+1}^{k}.$$

If $t = k - 1$, then this product is $\prod_{i=1}^k a_i$; otherwise,

$$\prod_{i=1}^{t} a_i(\prod_{j=t+1}^{k-1} \cdot a_k) = (\prod_{i=1}^{k} a_i \prod_{j=t+1}^{k-1}) \cdot a_k = (\prod_{i=1}^{k-1} a_i) \cdot a_k = \prod_{i=1}^{n} a_i.$$

3. We prove this claim by induction on n. If $n = 2$, according to $S_2 = \{(1), (12)\}$ and $a_1a_2 = a_2a_1$, hence the claim is true for $n = 2$. Assume that the claim is true for $n < k$. Let $n = k$, for any $\sigma \in S_k$, if $\sigma(k) = k$, then

$$a_{\sigma(1)}...a_{\sigma(k-1)}a_k = a_1...a_{k-1}a_k;$$

if $\sigma(i) = k$, and $i \neq k$, according to Exercise 1.1.2, then

$$\begin{aligned} a_{\sigma(1)}...a_{\sigma(k-1)}a_{\sigma(k)} &= (a_{\sigma(1)}...a_{\sigma(i-1)})(a_k \cdot a_{\sigma(i+1)}...a_{\sigma(k)}) \\ &= (a_{\sigma(1)}...a_{\sigma(i-1)})(a_{\sigma(i+1)}...a_{\sigma(k)} \cdot a_k) \\ &= (a_{\sigma(1)}...a_{\sigma(i-1)}a_{\sigma(i+1)}...a_{\sigma(k)}) \cdot a_k \\ &= a_1...a_{k-1}a_k. \end{aligned} \tag{1}$$

4. For any $a, b, c \in \mathbb{Z}$,

   (1) Associative:$(a \circ b) \circ c = (a + b - ab) \circ c = a + b + c - ab - ac - bc + abc$ and $a \circ (b \circ c) = (a + b - ab) \circ c = a + b + c - ab - ac - bc + abc$, hence $(a \circ b) \circ c = a \circ (b \circ c)$;

   (2) Identity:there exists $0 \in \mathbb{Z}$, s.t. $a \circ 0 = a = 0 \circ a$, hence 0 is the identity of $(\mathbb{Z}, \circ)$;

   (3) Commutative:$b \circ a = b + a - ba = a + b - ab = a \circ b$.

   Hence $(\mathbb{Z}, \circ)$ is a commutative monoid.

5. (1)For any $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in M$,

   (a) Associative:

   $$\begin{aligned} &((x_1, x_2)(y_1, y_2))(z_1, z_2) \\ =&(x_1y_1z_1 + 2x_2y_2z_1 + 2x_1y_2z_2 + 2x_2y_1z_2, x_1y_1z_2 + 2x_2y_2z_2 + x_1y_2z_1 + x_2y_1z_1) \end{aligned}$$

   and

   $$\begin{aligned} &(x_1, x_2)((y_1, y_2)(z_1, z_2)) \\ =&(x_1y_1z_1 + 2x_2y_2z_1 + 2x_1y_2z_2 + 2x_2y_1z_2, x_1y_1z_2 + 2x_2y_2z_2 + x_1y_2z_1 + x_2y_1z_1), \end{aligned}$$

   hence $((x_1, x_2)(y_1, y_2))(z_1, z_2) = (x_1, x_2)((y_1, y_2)(z_1, z_2))$.

   (b) Identity:There exists $(1, 0) \in M$, s.t.

   $$(1, 0)(x_1, x_2) = (x_1, x_2) = (x_1, x_2)(1, 0),$$

   hence $(1, 0)$ is the identity of M.

   (c) Commutative:$(y_1, y_2)(x_1, x_2) = (y_1x_1 + 2y_2x_2, y_1x_2 + y_2x_1) = (x_1, x_2)(y_1, y_2)$.

   (2)If $(x_1, x_2)(y_1, y - 2) = (x_1, x_2)(z_1, z_2)$, i.e.

   $$(x_1y_1 + 2x_2y_2, x_1y_2 + x_2y_1) = (x_1z_1 + 2x_2z_2, x_1z_2 + x_2z_1),$$

   then

   $$\begin{cases} x_1y_1 + 2x_2y_2 = x_1z_1 + 2x_2z_2 \\ x_1y_2 + x_2y_1 = x_1z_2 + x_2z_1 \end{cases}$$

i.e.
$$\begin{cases} x_1(y_1 - z_1) + 2x_2(y_2 - z_2) = 0 \\ x_2(y_1 - z_1) + x_1(y_2 - z_2) = 0 \end{cases}$$

since $\begin{vmatrix} x_1 & 2x_2 \\ x_2 & x_1 \end{vmatrix} = x_1^2 - 2{x_2}^2 \neq 0$, the equation has only one solution. Hence
$$\begin{cases} y_1 = z_1 \\ y_2 = z_2 \end{cases}$$

i.e. $(y_1, y_2) = (z_1 z_2)$.

6. (1)$\Rightarrow$:It is obvious.

   $\Leftarrow$:Since for any $b \in G$, there exists $c \in G$, s.t. $cb = e$. For any $a \in G$, then
   $$ab = eab = (cb)ab = c(ba)b = ceb = c(eb) = cb = e.$$

   Hence b is invertible. And $ae = a(ba) = ea = a$, hence e is an identity. Hence G is a group.

   (2)For example:$G = \{e, a, b\}$, for any $x, y \in G$, $xy = y$, then $ea = a, eb = b, e^2 = e$, and $ae = be = e^2 = e$, but G is not a group for e not satisfied $ae = a = ea$.

7. Since G is a group, there exists $c \in G$, s.t. $ca = e$, then
   $$ba = eba = (ca)ba = c(ab)a = ca = e.$$

   Hence $b = a^{-1}$.

8. Since
   $$\begin{pmatrix} E_m & -A \\ 0 & E_n \end{pmatrix}\begin{pmatrix} E_m & A \\ B & E_n \end{pmatrix}\begin{pmatrix} E_m & 0 \\ -B & E_n \end{pmatrix} = \begin{pmatrix} E_m - AB & 0 \\ 0 & E_n \end{pmatrix}$$

   and
   $$\begin{pmatrix} E_m & 0 \\ -B & E_n \end{pmatrix}\begin{pmatrix} E_m & A \\ B & E_n \end{pmatrix}\begin{pmatrix} E_m & -A \\ 0 & E_n \end{pmatrix} = \begin{pmatrix} E_m & 0 \\ 0 & E_n - BA \end{pmatrix}.$$

   Hence $E_m - AB$ is invertible if and only if $E_n - BA$ is invertible.

9. (1)$\Rightarrow$:If $a + \mathbb{Q} = b + \mathbb{Q}$, then there exists $x, x' \in \mathbb{Q}$, s.t. $a + x = b + x'$. Since $(\mathbb{Q}, +)$ is a group, $a - b = x' - x \in \mathbb{Q}$.

   $\Leftarrow$:If $a - b \in \mathbb{Q}$, then there exists $y \in \mathbb{Q}$, s.t. $a - b = y$, hence $b = a - y$, i.e. $b \in a + \mathbb{Q}$. Hence $b + \mathbb{Q} \subset a + \mathbb{Q}$. For the same reason, $a + \mathbb{Q} \subset b + \mathbb{Q}$. Hence $a + \mathbb{Q} = b + \mathbb{Q}$.

   (2)If $a + \mathbb{Q} = a' + \mathbb{Q}$, and $b + \mathbb{Q} = b' + \mathbb{Q}$, then $a' = a + x, b' = b + x'$ for some $x, x' \in \mathbb{Q}$. Thus, $(a' + b') = (a + b) + x + x'$. Since $x + x' \in \mathbb{Q}$, $(a + b) + \mathbb{Q} = (a' + b') + \mathbb{Q}$.

   (3)For any $a + \mathbb{Q}, b + \mathbb{Q}, c + \mathbb{Q} \in \mathbb{R}/\mathbb{Q}$,

(a) Associative:

$$((a+\mathbb{Q})+(b+\mathbb{Q}))+(c+\mathbb{Q}) = (a+b+c)+\mathbb{Q} = (a+\mathbb{Q})+((b+\mathbb{Q})+(c+\mathbb{Q}));$$

(b) Identity:there exists $0+\mathbb{Q} \in \mathbb{R}/\mathbb{Q}$, s.t.

$$(0+\mathbb{Q}) + (a+\mathbb{Q}) = (a+\mathbb{Q}) = (a+\mathbb{Q}) + (0+\mathbb{Q});$$

(c) Invertible:there exists $-a+\mathbb{Q} \in \mathbb{R}/\mathbb{Q}$, s.t.

$$(-a+\mathbb{Q}) + (a+\mathbb{Q}) = 0+\mathbb{Q} = (a+\mathbb{Q}) + (-a+\mathbb{Q});$$

(d) Commutative:$(a+\mathbb{Q}) + (b+\mathbb{Q}) = (a+b)+\mathbb{Q} = (b+\mathbb{Q}) + (a+\mathbb{Q})$.

Hence $(\mathbb{R}/\mathbb{Q}, +)$ is an abelian group.

10. If $m, n \geq 0$, if $n = 1$, we have $a^m a^0 = a^{m+0}$.If $n = 1$, according to the definition, we have $a^m a = a^{m+1}$. Assume that it is true for $n < k$, let $n = k$, then $a^m a^n = a^m(a^{n-1}a) = a^{m+n-1}a = a^{m=n}$ by induction on n. For the same reason, it is true for $m < 0, n \geq 0$. If $m, n \leq 0$,Since $a^{-n} = (a_n)^{-1}$, $a^m a^n = (a^{-n}a^{-m})^{-1} = (a^{-m-n})^{-1} = a^{m+n}$. For the same reason, it is true for $m \geq 0, n < 0$.

11. We prove this formula by induction on n. If $n = 2$, then $(ab)^2 = ab \cdot ab = a(ba)b = a^2b^2$, hence the claim is true for $n = 2$. Assume that the claim is true for $n = k$. Let $n = k+1$, $(ab)^{k+1} = (ab)^k \cdot (ab) = a^k(b^k a)b = (a^k a)(b^k b) = a^{k+1}b^{k+1}$.

No. For example:In $GL(\mathbb{Z}, \mathbb{P})$, $a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

$$ab = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = ba,$$

$$(ab)^n = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}^n = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^n \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \frac{-1+(-1)^n}{2} \\ 0 & (-1)^n \end{bmatrix},$$

$$a^n b^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^n \end{bmatrix} = \begin{bmatrix} 1 & (-1)^n n \\ 0 & (-1)^n \end{bmatrix}.$$

Hence $(ab)^n \neq a^n b^n$.

12. (1)$\Rightarrow$(2):$(ab)^2 = a(ba)b = a(ab)b = a^2b^2$,

(2)$\Rightarrow$(1):If $abab = a^2b^2$, then $ba = ab$.

(1)$\Rightarrow$(3):Since $ab = ba$ for all $a, b \in G$, $(ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$,

(3)$\Rightarrow$(1):Since $b^{-1}a^{-1} = (ab)^{-1} = a^{-1}b^{-1}$,

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

(1)$\Rightarrow$(4):According to Exercise 1.1.11.

(4)$\Rightarrow$(1):If $(ab)^n = a^n b^n, (ab)^{n+1} = a^{n+1}b^{n+1}, (ab)^{n+2} = a^{n+2}b^{n+2}$,

then $(ab)^{n+1} = ab \cdot (ab)^n = aba^n b^n = a^{n+1}b^{n+1}$, thus, $ba^n = a^n b$;

and $(ab)^{n+2} = (ab)^2 \cdot a^n b^n = ababa^n b^n = a^{n+2}b^{n+2}$,

thus, $baba^n = a^{n+1}b^2 = ba^{n+1}b$; then $ba^{n+1}b = a^{n+1}b = ba^n \cdot a = a^n ba$, hence $ab = ba$.

For example:In S_3, $a = (12), b = (23)$, then $(ab)^6 = (123)^6 = (1) = a^6 b^6$ and $(ab)^7 = (123) = a^7 b^7$, but $ab = (123) \neq (132) = ba$.

13. If $ord(a) > 2$, then $ord(a^{-1}) > 2$. Thus, there are even elements which order is large than 2. Hence $B = \{x \in G||x| = n, n \leq 2\}$ has even elements. Since $ord(e) = 1$, there exists $b \in G$ s.t. $b^2 = e$.

14. Let $K = \{x^{-1}|x \in H\}$. Since $a = b$, $a^{-1} = b^{-1}$, thus $|K| = |H|$. Hence, $aK = \{ax|x \in K\}$ for any $a \in G$, then $|aK| = |K|$. Since $|aK|+|H| > |G|$, $aK \cap H \neq \emptyset$. Assume that $a{h_1}^{-1} = h_2 \in aK \cap H$, then $a = h_1 h_2$. Hence each elements of G is a product of two elements in H.

15. $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (253)$.

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (132)$.

Since $\tau^6 = (1)$, $\tau^{-1} = \tau^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$.

Then $\tau^{-1}\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (135)(24)$.

16. (1)Since $X \subset X$, $2^X \neq \emptyset$. For any elements $A, B, C \in 2^X$,

    (a) Associative:$(A \triangle B) \triangle C = A \cup B \cup C - A \cap B - A \cap C - B \cap C + A \cap B \cap C$, while $A \triangle (B \triangle C) = A \cup B \cup C - A \cap B - A \cap C - B \cap C + A \cap B \cap C$. Hence $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

    (b) Identity:There exists $\emptyset \in 2^X$ s.t. $A \triangle \emptyset = A = \emptyset \triangle A$.

    (c) Invertible: Since $A \triangle A = \emptyset$, A is the inverse of A.

    Hence 2^X is a group .

    (2)If $|X| = n$, then there are C_n^k subsets of k elements. Hence there are $C_n^0 + C_n^1 + \cdots + C_n^n = 2^n$ subsets, i.e. $|2^X| = 2^n$.

17. $S(A) = \{t^n|n \in \mathbb{Z}^+\}$ is a semigroup.

    $M(A) = \{t^n|n \in \mathbb{N}\}$ is a monid.

    $F(A) = \{t^n|n \in \mathbb{Z}\}$ is a group.