II.C. Groups and subgroups

Some further simple properties follow from the defining properties:

II.C.1. **Proposition.** Let $G$ be a group, and $a, b, x \in G$.  
(a) The cancellation laws hold: $xa = xb$ (or $ax = bx$) $\implies a = b$.  
(b) The inverse of $x$ is unique, and $(x^{-1})^{-1} = x$.  
(c) $(a^n)^m = a^{nm}$, $a^ma^n = a^{m+n}$ [laws of exponents]  
(d) If $a$ and $b$ commute $(ab = ba)$, then $(ab)^n = a^n b^n$.  

**Proof.** (a) Multiply on the left (resp. right) by $x^{-1}$.  
(b) If $x' x = 1 = xx'$ and $x'' x = 1 = xx''$, then  
$$x'' = x''1 = x''xx' = 1x' = x'.$$
(c) Clear from the definition: $a^n = a \cdots a$ ($n$ times).  
(d) If $a$ commutes with $b$, it commutes with powers of $b$. Now induce on $n$:  
$$(ab)^n = (ab)^{n-1}ab = a^{n-1}b^{n-1}ab = a^{n-1}ab^{n-1}b = a^n b^n.$$  
\[\square\]

II.C.2. **Remark.** (i) $ab = ba$ is equivalent to the triviality of the **commutator** $[a, b] := a^{-1}b^{-1}ab$. (In algebra, an element being *trivial* means it’s the identity element.)  
(ii) For monoids: (a) is false, (c) and (d) hold. For those elements of the monoid that have a (two-sided) inverse, (b) is true. (But those elements form a group, so this doesn’t say much...)

II.C.3. **Examples.** (i) **Abelian groups:**  
- $(A, +, 0)$ where $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.  
- $(V, +, 0)$ where $V$ is a vector space.  
- $(\mathbb{Z}_n, +, 0)$ where $\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \text{integers mod } n$.  
- $(\mathbb{Z}_n^*, \cdot, 1)$ where $\mathbb{Z}_n^* \subset \mathbb{Z}_n$ is the subset of elements possessing a multiplicative inverse: $\bar{b} \in \mathbb{Z}_n$ such that $\bar{a} \bar{b} = \bar{1}$.  
- $(\mathbb{A}_*, \cdot, 1)$ where $\mathbb{A}_* = \mathbb{Q}_*, \mathbb{R}_*, \mathbb{C}_*$ (here $\mathbb{Q}_* = \mathbb{Q} \setminus \{0\}$ etc.).  
- $\{1, -1\}, \cdot, 1$, and more generally $(\{e^{2\pi ik}\}_{k=0}^{n-1}, \cdot, 1)$.  
- rotational symmetries of the (regular) $n$-gon.  

Notes: (a) $\mathbb{Z}_n^* = \{\bar{a} \mid (a, n) = 1\}$, since (by I.B.4) $(a, n) = 1 \iff \exists b, k \in \mathbb{Z}$ with $ab + nk = 1 \iff \exists b$ such that $\bar{a} \bar{b} = \bar{1}$.  

(b) $\mathbb{Z}_n$ is an example of a **cyclic group**; i.e. a group on one generator: the notation

$$\mathbb{Z}_n = \langle \bar{1} \mid n \cdot \bar{1} = 0 \rangle$$

means that the elements comprise all of the “powers” $0, 1, 1 + 1, 1 + 1 + 1, \text{etc.}$ of the generator $\bar{1}$, subject to the relation shown ($n \cdot \bar{1} = \bar{1} + \cdots + \bar{1}$ [n times] = 0). $\mathbb{Z} = \langle 1 \rangle$ is also a cyclic group (with no relation), but (unlike $\mathbb{Z}_n$) an infinite one.

(ii) **Non-abelian groups**:

- $S_n$ = *n*th symmetric group, for $n \geq 3$.
- $D_n$ = *n*th **dihedral group**, for $n \geq 3$: its elements comprise the rotational and reflectional symmetries of a regular *n*-gon.
- $GL_n(A)$ **general linear group**, for $n \geq 2$ (and $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$): elements are invertible $n \times n$ matrices with entries in $A$.
- $SL_2(\mathbb{Z})$ (integer $2 \times 2$ matrices with determinant 1) and other “arithmetic groups”.

**Notes**: As suggested in (i), it can be useful to write groups in terms of **generators** and **relations**. For instance, for the “quotient of $SL_2(\mathbb{Z})$” by $\pm \left( \begin{array}{ll} 1 & 0 \\ 0 & 1 \end{array} \right)$, $PSL_2(\mathbb{Z}) = \langle S, R \mid S^2 = 1 = R^3 \rangle$ where

$$\begin{align*}
S &= \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right) \\
R &= \left( \begin{array}{cc} 0 & -1 \\ 1 & 1 \end{array} \right) = S \cdot \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)
\end{align*}$$

says that the elements of $PSL_2(\mathbb{Z})$ are arbitrary “words” in $S$ and $R$ (and their inverses) subject only to the two relations written. For the dihedral group, we have

$$D_n = \langle r, h \mid \text{relations are a HW exercise!} \rangle$$

where $r$ is counterclockwise rotation by $\frac{2\pi}{n}$ and $h$ is a choice of reflection. We have also shown that $S_n$ is generated by transpositions.

(iii) **Monoids that are not groups**:

- $(\mathbb{N}, +, 0)$, $(\mathbb{Z}_{>0}, \bullet, 1)$, or $(\mathbb{Z} \setminus \{0\}, \bullet, 1)$. 


• \((\mathcal{P}(S), \cup, \emptyset)\) for any nonempty set \(S\).
• \((\sigma, +, (0, 0))\) where \(\sigma\) is a cone in \(\mathbb{R}^2\):

![Diagram of a cone](image)

• the monoid of integral ideals in an algebraic number ring (which we will meet later).

(iv) **Direct products of (monoids or) groups:** \(G_1 \times G_2\), with group operation 
\((g_1, g_2) \cdot (h_1, h_2) := (g_1 h_1, g_2 h_2)\).

**II.C.4. Definition.** A **subgroup** of \(G\) is a subset \(H \subset G\) satisfying:
(i) \(1_G \in H\);
(ii) [closure under multiplication] \(x, y \in H \implies xy \in H\); and
(iii) [closure under inversion] \(x \in H \implies x^{-1} \in H\).
We write \(H \leq G\) (or \(H < G\) for a proper subgroup — i.e. \(H \neq G\)), and endow \(H\) with the operation “•” inherited from \(G\) (and hence with a group structure).

**II.C.5. Examples.** (a) When \(a \in G\) is an element of a group, we will use the notation \(\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}\) to denote the **cyclic subgroup** generated by \(a\). (Though no relation is written, this can certainly be finite since some power of \(a\) may be 1 in \(G\).) Cyclic subgroups are clearly abelian.

(b) In \(D_n\), we have cyclic subgroups \(\langle r \rangle < D_n\) (resp. \(\langle h \rangle\)) of order \(n\) (resp. 2). In \(\mathbb{C}^*\), \(\langle e^{\frac{2\pi i}{n}} \rangle\) is the (cyclic) group of \(n^{th}\) roots of unity. We can intuitively think of \(\langle e^{\frac{2\pi i}{n}} \rangle\) and \(\langle r \rangle\) as copies of \((\mathbb{Z}_n, +, 0)\) embedded in \(\mathbb{C}^*\) and \(D_n\), but we’ll need to employ homomorphisms and isomorphisms to state this properly.)
(c) Intersections of subgroups are again subgroups: given \( H, K \leq G \), we have \( H \cap K \leq G \). (Why?)

(d) Generalizing (a), we can consider subgroups generated by a subset \( S \subset G \), denoted \( \langle S \rangle \leq G \). There are three equivalent definitions of this: as the smallest subgroup of \( G \) containing \( S \); as the intersection of all subgroups containing \( S \); or as all products of (powers of) elements of \( S \) and their inverses.

(e) The centralizer of a subset \( S \subset G \) is defined by

\[
C_G(S) := \{ g \in G \mid gs = sg \; (\forall s \in S) \} \leq G.
\]

(To see that it is a subgroup, rewrite the condition in the braces as \( sgs^{-1} = g \). If also \( sg' s^{-1} = g' \), then \( s(gg')s^{-1} = (sgs^{-1})(sg's^{-1}) = gg' \), and \( sg^{-1}s^{-1} = (sgs^{-1})^{-1} = g^{-1} \).) In particular, we write \( C_G(a) := C_G(\{a\}) \) for the centralizer of one element, and \( C(G) := C_G(G) \) for the center of \( G \). (Often “\( C \)” is written “\( Z \)” — this is the German heritage.)

(f) The cone in II.C.3(iii) is a submonoid of \( \mathbb{R}^2 \).

(g) A submonoid of \( \mathcal{S}_X \) is called a monoid of transformations of \( X \). A subgroup of \( \mathcal{S}_X \) is a group of permutations of \( X \). Here is an interesting example.

Define \( \mathcal{A}_n \subset \mathcal{S}_n \) by

\[
\mathcal{A}_n := \{ \alpha \in \mathcal{S}_n \mid \alpha \text{ is even} \} = \{ \alpha \in \mathcal{S}_n \mid \text{sgn}(\alpha) = 1 \}.
\]

We claim that, since \( \text{sgn} \) is a homomorphism, this is a subgroup: indeed, \( 1 \in \mathcal{A}_n \), and given \( \alpha, \beta \in \mathcal{A}_n \),

\[
\text{sgn}(\alpha) = 1 = \text{sgn}(\beta) \implies \begin{cases} 
\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta) = 1 \\
\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha)^{-1} = 1
\end{cases}
\]

so that (ii), (iii) in II.C.4 hold. This subgroup \( \mathcal{A}_n \leq \mathcal{S}_n \) is called the alternating group.

II.C.6. PROPOSITION. If \( n \geq 3 \), \( \mathcal{A}_n \) is generated by 3-cycles.
II.C. GROUPS AND SUBGROUPS

PROOF. \( \alpha \in \mathfrak{A}_n \implies \alpha \) is a product of an even number of transpositions. We can group these into pairs of distinct transpositions, viz. \( \alpha = (\tau_1 \tau_2) \cdots (\tau_{2q-1} \tau_{2q}) \). For a pair \( \tau \tau' \), if the transpositions are not disjoint, write

\[
(ij)(ik) = (ikj);
\]

while if they are disjoint, write

\[
(ij)(k\ell) = (ij)(jk)(j\ell) = (ijk)(j\ell).
\]

This recasts \( \alpha \) as a product of 3-cycles. (That, conversely, all 3-cycles belong to \( \mathfrak{A}_n \) is clear from the first displayed formula.) \( \square \)