Basic Algebraic Terminology

Definition. A semigroup \((S, \circ)\) is a nonempty set \(S\) together with an associative binary operation \(\circ\) on it, i.e. \(a \circ (b \circ c) = (a \circ b) \circ c\) for all \(a, b, c \in S\).

Remark. In the following, \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\) denote the sets of integers, rational numbers, real numbers, complex numbers, respectively. For a positive integer \(n\), \(\mathbb{Z}/n\mathbb{Z}\) denotes the set of residue classes of \(\mathbb{Z}\) modulo \(n\), and \((\mathbb{Z}/n\mathbb{Z})^\times\) denotes the set equivalence classes which are relatively prime to \(n\). For a prime number \(p\), \(\mathbb{Z}_p\) denotes the set of \(p\)-adic integers, and \(\mathbb{Q}_p\) the set of \(p\)-adic numbers. Finally, \(M_2(\mathbb{R})\) denotes the set of 2x2 matrices with entries in \(\mathbb{R}\), and \(GL_2(\mathbb{R})\) denotes the set of 2x2 matrices with nonzero determinant.

Example.
- The sets \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}_p, M_2(\mathbb{R})\) with their usual addition operations are semigroups.
- The sets \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^\times, \mathbb{Z}_p, \mathbb{Q}_p, M_2(\mathbb{R}), GL_2(\mathbb{R})\) with their usual multiplication operations are semigroups.

Definition. A monoid \((M, \circ, e)\) is a semigroup \((M, \circ)\) together with an identity element \(e \in M\), i.e. \(e \circ a = a = a \circ e\) for all \(a \in M\).

Remark. If a semigroup has an identity element, then it is unique. If \(e_1\) and \(e_2\) are two identity elements, then \(e_1 = e_1 \circ e_2 = e_2\).

Example. The semigroups in the first example are also monoids. The set of positive integers with addition is a semigroup which is not a monoid.

Definition. Let \((M, \circ, e)\) be a monoid. An element \(a \in M\) is a unit if there exists \(b \in M\) such that \(a \circ b = e = b \circ a\). \(U(M, \circ, e)\) or just \(U(M, \circ)\) will denote the set of units of \((M, \circ, e)\) in the following.

Example.
- \(U(M, +) = M\) if \(M\) is \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}_p, M_2(\mathbb{R})\).
- \(U(M, \cdot) = M - \{0\}\) if \(M\) is \(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p\).
- \(U(\mathbb{Z}, \cdot) = \{1, -1\}\).
- \(U(\mathbb{Z}/n\mathbb{Z}, \cdot) = (\mathbb{Z}/n\mathbb{Z})^\times\).
- \(U(M_2(\mathbb{R}), \cdot) = GL_2(\mathbb{R})\).
- \(U(\mathbb{Z}_p, \cdot) = \{x \in \mathbb{Z}_p : p \nmid x\}\).

Definition. A group \((M, \circ, e)\) is a monoid with \(U(M, \circ) = M\).

Example.
- \((M, +)\) is a group if \(M\) is \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}_p, M_2(\mathbb{R})\).
- \((M - \{0\}, \cdot)\) is a group if \(M\) is \(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p\).
- In general, for any monoid \((M, \circ, e)\), \(U(M, \circ)\) is a group.
• \((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\) and \((GL_2(\mathbb{R}), \cdot)\) are groups.
• In general, for any monoid \((M, \circ, e), U(M)\circ)\) is a group.

**Definition.** A semigroup, monoid or group is **commutative** if its binary operation is commutative, i.e. \(a \circ b = b \circ a\) for all \(a, b\).

**Example.** Of the examples above only \((M_2(\mathbb{R}), \cdot)\) and \((GL_2(\mathbb{R}), \cdot)\) are not commutative.

**Definition.** A ring \((R, +, \cdot, 0, 1)\) is a commutative group \((R, +, 0)\) and a monoid \((R, \cdot, 1)\) such that \(a \cdot (b + c) = a \cdot b + a \cdot c\) and \((b + c) \cdot a = b \cdot a + c \cdot a\) for all \(a, b, c \in R\).

A ring is **commutative** if \((R, \cdot, 1)\) is commutative.

\(U(R, \cdot, 1)\) is the **group of units** of the ring \(R\).

A commutative ring with \(0 \neq 1\) and \(U(R, \cdot, 1) = R - \{0\}\) is a **field**.

**Example.**
- \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}_p, M_2(\mathbb{R})\) with their usual addition and multiplication operations are rings.
- \(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p\) are fields.
- If \(p\) is a prime number, then \(\mathbb{Z}/p\mathbb{Z}\) is a field.

**Definition.** Let \((M, \circ, e)\) and \((M', \circ', e')\) be monoids. A function \(f : M \to M'\) is a **monoid homomorphism** if \(f(a \circ b) = f(a) \circ' f(b)\) for all \(a, b \in M\) and \(f(e) = e'\).

\(f\) is a **monoid isomorphism** if it is also a bijection, that is, one-to-one and onto.

The homomorphisms and isomorphisms of the other algebraic structures above are defined in a similar manner.

**Example.**
- The inclusion function \(f : \mathbb{Z} \to \mathbb{Q}\) is a ring homomorphism.
- The function \(f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\) which sends each integer to its equivalence class modulo \(n\) is a ring homomorphism.
- If \(m|n\), then the function \(f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}\) which sends each equivalence class modulo \(n\) to the corresponding equivalence class modulo \(m\) is a ring homomorphism.
- The inclusion function \(f : \mathbb{Q} \to \mathbb{R}\) is a field homomorphism.

**Example.** There is a unique group homomorphism \(f : (\mathbb{Z}/6\mathbb{Z}, +) \to (\mathbb{Z}/7\mathbb{Z}, \cdot)\) which satisfies \(f(1) = 3\). This is in fact a group isomorphism.

**Example.** For \(a, b \in \mathbb{Z}\), let
\[
f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}
\]
Then \(f : \mathbb{C} \to M_2(\mathbb{R})\) is a ring homomorphism.

**Definition.** Let \((M_1, \circ_1, e_1)\) and \((M_2, \circ_2, e_2)\) be monoids. A binary operation \(\circ\) on the Cartesian product set \(M_1 \times M_2 = \{(m_1, m_2) : \)

$m_1 \in M_1, m_2 \in M_2 \}$ is defined by $(a_1, a_2) \circ (b_1, b_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2)$.
Then $(M_1 \times M_2, \circ_1, (e_1, e_2))$ is the direct product monoid of the monoids $(M_1, \circ_1, e_1)$ and $(M_2, \circ_2, e_2)$.

The direct product monoid is in fact a monoid. Direct products of semigroups, groups and rings are defined similarly.

Example. Let $n = n_1 n_2 \cdots n_r$ where $\gcd(n_i, n_j) = 1$ for $i \neq j, 1 \leq i, j \leq r$. Then the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ whose existence and uniqueness is essentially the statement of the Chinese Remainder Theorem, and which is constructed in the proof of the theorem is in fact a ring isomorphism.

Example. In general, a ring isomorphism gives a group isomorphism when restricted to the groups of units of the corresponding rings. So the Chinese Remainder Theorem also implies that the groups $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$ are isomorphic.

A Closer Look at the Groups

Definition. A group is an ordered triple $(G, \circ, e)$ where $G$ is a nonempty set, $e$ is an element of $G$ and $\circ$ is a binary operation on $G$ such that:

- $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$,
- $e \circ a = a = a \circ e$ for every $a \in G$,
- for every $a \in G$, there exists $b \in G$ such that $a \circ b = e = b \circ a$.

The element $e$ is the identity element of the group. For a given $a \in G$, the element $b$ whose existence is guaranteed in the last condition is unique and is the inverse of $a$. It is denoted by $a^{-1}$.

Remark. Of course the notation for the inverse of $a$ conforms with the one used for “multiplication type” operations, and care should be exercised when using it for the “addition type” operations. This is also true for the following conventions.

From now on $a \circ b$ is written simply as $ab$. For an integer $n$, $a^n$ will stand for $a \circ a \circ \cdots \circ a$ with $n$ factors of $a$ if $n$ is positive, $(a^{-1})^{-n}$ if $n$ is negative, and $e$ if $n$ is 0.

Therefore in $(\mathbb{Z}, +)$, $3^{-1}$ means $-3$, and $3^5$ means 15.

Definition. Let $(G, \circ, e)$ be a group and let $H$ be a nonempty subset of $G$. If for all $a, b \in H$, $ab^{-1}$ is in $H$, then $H$ is a subgroup of $G$. In fact $H$ becomes a group with the restriction of $\circ$ and the same identity element $e$ as $G$.

Example. For a positive integer $n$, let $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$. Then $\mu_n$ is a group with the usual multiplication of complex numbers. If $m|n$, then $\mu_m$ is a subgroup of $\mu_n$. 
Example. Let $SL_2(\mathbb{R}) = \{g \in GL_2(\mathbb{R}) : \det g = 1\}$. Then $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

Example.

$$G = \begin{Bmatrix} 1 & 0, & -1 & 0, & i & 0, & -i & 0, \\ 0 & 1, & 0 & -1, & 0 & i, & 0 & i, \\ -1 & 0, & 1 & 0, & 0 & 0, & 0 & -i, \\ 0 & -1, & 1 & 0, & 0 & 0, & 0 & i \end{Bmatrix}$$

is a group under the usual multiplication operation of matrices. Then

$$H = \begin{Bmatrix} 1 & 0, & -1 & 0, & i & 0, & -i & 0, \\ 0 & 1, & 0 & -1, & 0 & i, & 0 & i, \\ -1 & 0, & 1 & 0, & 0 & 0, & 0 & -i, \\ 0 & -1, & 1 & 0, & 0 & 0, & 0 & i \end{Bmatrix}$$

is a subgroup of $G$.

For a finite set $S$, $|S|$ denotes the number of elements of $S$.

Theorem. Let $G$ be a finite group, and let $H$ be a subgroup of $G$. Then $|H| | |G|.$

Proof. For $g \in G$, let $gH = \{gh : h \in H\}$. Then for $g_1, g_2 \in G$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$: If $g \in g_1H \cap g_2H$, then there are $h_1, h_2 \in H$ such that $g_1h_1 = g = g_2h_2$. This implies that $g_2 = g_1h_1h_2^{-1}$ and $g_2h = g_1(h_1h_2^{-1})h \in g_1H$ for all $h \in H$. Hence $g_2H \subseteq g_1H$. A similar argument gives $g_1H \subseteq g_2H$. Therefore $g_1H = g_2H$.

Since $g \in gH$ for every $g \in G$, $G = \bigcup_{g \in G} gH$. As the sets in the union are either disjoint or identical, there exists a positive integer $r$ and $g_1, \ldots, g_r \in G$ such that $G$ is the disjoint union of $g_1H, \ldots, g_rH$. Then $|G| = \sum_{k=1}^r |g_kH| = \sum_{k=1}^r |H| = r|H|$. Then $|G| / |H| = r \in \mathbb{Z}$. \hfill \Box

Theorem. Let $g \in G$. Assume that there exists a nonzero integer $m$ such that $g^m = e$. Then there exists a positive integer $n_0$ such that $g^n = e \quad \iff \quad n \equiv 0 [n_0]$.\hfill \Box

Proof. Let $S = \{n \in \mathbb{Z} : g^n = e\}$. Then by assumption $S$ is not empty. As $m \in S \implies -m \in S$, it contains at least one positive integer. Let $n_0$ be the smallest positive integer in $S$. Then $S = \{kn_0 : k \in \mathbb{Z}\}$.

That $S \supset \{kn_0 : k \in \mathbb{Z}\}$ is obvious. On the other hand, if $n \in S$, let $n = qn_0 + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n_0$. $e = a^n = a^{qn_0+r} = (a^{n_0})^qa^r = a^r$.

Contradicts $n_0$ being the smallest positive integer in $S$ unless $r = 0$, i.e. $n \equiv 0 [n_0]$. \hfill \Box

Definition. Let $g \in G$. The smallest positive integer $n$ such that $g^n = e$, if it exists, is called the order of $g$ and denoted by ord $g$.

Example. $(1 + \sqrt{3}i)/2 \in \mu_6$ has order 6 whereas $(-1 + \sqrt{3}i)/2$ has order 3 and $-1$ has order 2.

Example.

- In $(\mathbb{Z}/12\mathbb{Z}, +)$, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 have orders 1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12, respectively.
• In \((\mathbb{Z}/13\mathbb{Z}, +)\), 0 has order 1, and all the other elements have order 13.

**Example.**
• In \((\mathbb{Z}/7\mathbb{Z})^\times\), 1, 2, 3, 4, 5, 6 have orders 1, 3, 6, 3, 6, 2, respectively.
• In \((\mathbb{Z}/8\mathbb{Z})^\times\), 1 has order 1, and 3, 5, 7 have order 2.

**Remark.** A simple pigeonhole principle argument shows that the order of every element of a finite group is defined.

**Theorem (Lagrange).** Let \(G\) be a finite group. Then for every \(g \in G\), \(\text{ord } g | |G|\).

**Proof.** Let \(d = \text{ord } g\) and \(H = \{g^k : 1 \leq k \leq d\}\). Then \(H\) is a subgroup of \(G\). Hence \(\text{ord } g = |H|||G|\). \(\square\)

**Definition.** Let \(G\) be a finite group. \(G\) is cyclic and \(g \in G\) is a generator of \(G\) if \(G = \{g^k : 1 \leq k \leq d\}\) where \(d = \text{ord } g\).

**Example.** \(\mu_n\) is a cyclic group. \(\cos(2\pi/n) + \sin(2\pi/n)i\) is a generator of \(\mu_n\). In fact, \(\cos(2\pi k/n) + \sin(2\pi k/n)i\) is a generator for every integer \(k\) with \(\gcd(k, n) = 1\).

**Example.** \((\mathbb{Z}/n\mathbb{Z}, +)\) is a cyclic group for every \(n\). Every integer \(k\) with \(\gcd(k, n) = 1\) is a generator.

**Example.** \((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\) is a cyclic group if and only if \(n = 2, 4, p^e\) or \(2p^e\) where \(p\) is an odd prime and \(e \geq 1\).

**Further reading:**
• I. N. Herstein, *Topics in Algebra*, Wiley (1975)