Contents

1 Group

1.1 Monoids

We call a mapping $S \times S \to S$ a law of composition. The image of the pair (x, y) is called their product or sum.
Let S be a set with a law of composition, and x, y, z be elements of S. Then we can form their product in the ways: $(xy)\, z$ or $x\,(yz)$. If $(xy)\, z = x\,(yz)$ for all $x, y, z \in S$, then the law of composition is **associative**.
We call the element e of S is **unit element** if e such that $ex = x = xe$ for all $x \in S$. When the law of composition is additive, the unit element is denoted by 0 and is called **zero element**.And the unit element is unique, so if e' is another unit element, we have $e = ee' = e'$.

Def 1. A **monoid** is a set G, with a law of composition which is associative, and having a unit element(in particular, G is not empty).

For instance, we can consider maps $f : S \times S \to T$ and $g : A \times B \times C \to D$. **Commutativity** means $f\,(x, y) = f\,(y, x)$ for all $x, y \in S$, and **associativity** means that $(ab)\, c = a\,(bc)$ for all $a \in A, b \in B, c \in C$. And if the law of composition of G is commutative, we also call that G is **commutative** or **abelian**.

Prop 1. Let G be a commutative monoid, and $x_1, \cdots, x_n$ elements of G. Let ψ be a bijection of the set of integers $(1, \cdots, n)$ onto itself Then $\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu$.

Proof. We can prove it by induction. And we only need to know for all $x_1, \cdots, x_n$

$$\begin{aligned}\prod_{1}^{n} x_{\psi(\nu)} &= \prod_{1}^{k} x_{\psi(\nu)} \cdot x_{\psi(\nu)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} \\ &= \prod_{1}^{k} x_{\psi(\nu)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} \cdot x_{\psi(k)}\end{aligned}$$

□

Cor 1. Let G be a commutative monoid, I be a set, and let $f : I \to G$ be a mapping such that $f\,(i) = e$ for almost all $i \in I$. Let I_0 be the subset of I consisting of those i such that $f\,(i) \neq e$. Then the product $\prod_{i \in I} f\,(i)$ is defined as $\prod_{i \in I_0} f\,(i)$. In particular, the empty product is equal to e.(If G is additive, the empty sum is equal to 0)

Cor 2. Let I, J be two sets, and $f : I \times J \to G$ a mapping into a commutative monoid which takes the value e for almost all pairs (i, j), we have $\prod_{i \in I} \left[\prod_{j \in J} f\,(i, j) \right] = \prod_{j \in J} \left[\prod_{i \in I} f\,(i, j) \right]$.

If S, S' are two subsets of a monoid G, then we define SS' to be the subset consisting of all elements xy, with $x \in S$ and $y \in S'$. And inductively, we can define the product od a finite number of subsets, and we have associativity.

Def 2. A submonoid of G is a subset H of G containing the unit element, and such that if $x, y \in H$ then $xy \in H$(We say that H is **closed** under the law of composition). It is clear that H is also a monoid.

1.2 Group

Def 3. A **group** G is a monoid, such that for every element $x \in G$ there exists an element $y \in G$ such that $xy = yx = e$. Such an element y is called an **inverse** for x. Similar to unit element, the inverse is also unique, because if y' is also an inverse for x, then $y' = y'e = y'(xy) = (y'x)y = ey = y$. We denote this inverse by x^{-1} (or $-x$ when the law of composition is additive).

We could also define left units and left inverses obviously. And it's easily to prove that these are also units and inverses respectively under suitable conditions. We can prove a set with an associative law of composition G is a group if G has a left unit for the law and a left inverse for every elements. Let $a \in G$ and $b \in G$ be such that $ba = e$, then $bab = eb = b$. Multiplying on the left by a left inverse for b yields $ab = e$, in other words, b is also a right inverse for a, and a is a left inverse for b.

e.g. 1. Let S be a non-empty set, and G be the set of bijective mappings of S onto itself. Then G is a group, the law of composition being ordinary composition of mappings. The unit element of G i the identity map of S, and the other group properties are trivially verified. The elements of G are called **permutations** of S. We also denote G by $\mathbf{Perm}(S)$.

e.g. 2. Let k be a field and V a vector space over k. Let $GL(V)$ denote the set of invertible $k-$linear maps of V onto itself. Then $GL(V)$ is a group under composition of mappings. Similarly, let k be a field and let $GL(n,k)$ be the set of invertible $n \times n$ matrices with components in k. Then $GL(k)$ is a group under the multiplication of matrices. For $n \geq 2$, this group is **not** commutative.

e.g. 3. (Direct product)
Let G_1, G_2 be groups. Let $G_1 \times G_2$ be the direct product as sets, so $G_1 \times G_2$ is the set of all pairs (x_1, x_2) with $x_i \in G_i$. We define the law of composition componentwise by $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2, y_2)$. Then $G_1 \times G_2$ is a group, whose unit element is (e_1, e_2) (where $e_i \in G_i$).

Def 4. A **subgroup** H of group G is a subset of G containing the unit element, and such that H is closed under the law of composition and inverse(on the other hand, it's a submonoid, such that if $x \in H$ then $x^{-1} \in H$). A subgroup is called **trivial** if it only consists of the unit element.

Def 5. Let G be a group and S a subset of G. We say that S generates G, or S is a set of **generators** for G, if every element of G can be expressed as a product of elements of S or inverses of elements of S. S generates G if and only if the smallest subgroup of G containing S is G itself. And we write $G = \langle S \rangle$ if G is generated by S.

Let G, G' be monoids. A **monoid-homomorphism** of G into G' is a mapping $f : G \to G'$ such that $f(xy) = f(x) f(y)$ for all $x, y \in G$, and mapping the unit element G into that of G'. And if G, G' are groups, it's a group-homomorphism.
Let $f : G \to G'$ be a group-homomorphism. Then $f\left(x^{-1}\right) = f(x)^{-1}$. Because if e, e' are the unit elements of G, G' respectively, then $e' = f(e) = f\left(xx^{-1}\right) = f(x) f\left(x^{-1}\right)$. Let G, G' be monoids. A homomorphism $f : G \to G'$ is called an isomorphism if there exists a homomorphism $g : G' \to G$ such that $f \circ g$ and $g \circ f$ are the identity mappings. It's trivially verified that f is an isomorphism if and only if f is bijective. And it's denoted by $G \simeq G'$. If $G = G'$, we say that isomorphism is an **automorphism**. A homomorphism of G into itself is also called an **endomorphism**.
Let $f : G \to G'$ and $g : G' \to G''$ be two group-homomorphisms. Then the composite map $g \circ f$ is a group-homomorphism. If f, g are isomorphisms then so is $g \circ f$. Furthermore $f^{-1} : G' \to G$ is also an isomorphism. In particular, the set of all automorphisms of G is itself a group, denoted by $Aut(G)$.
Let $f : G \to G'$ be a group-homomorphism and e, e' be the respective unit elements of G, G'. We define the **kernel** of f to be the subset of G consisting of all x such that $f(x) = e'$. H is closed under the inverse mapping. Let $x \in H$, then $f\left(x^{-1}\right) f(x) = f(e) = e'$. Since $f(x) = e'$, we have $f\left(x^{-1}\right) = e'$, whence $x^{-1} \in H$. Let H' be the **image** of f. Then H' is a subgroup of G', because it contains e', and

if $f(x), f(y) \in H$, then$f(xy) = f(x) f(y)$ lies also in H'.$f\left(x^{-1}\right) = f(x)^{-1}$ is in H', hence H' is a subgroup of G'. The kernel and image of f are denoted by $Kerf$ and Imf. A homomorphism $f : G \to G'$ which establishes an isomorphism between G and its image in G' will also be called an **embedding**.

Prop 2. A homomorphism whose kernel is trivial is injective.

参考文献