§0a Background material on group theory

The second part of the course on the fundamental group makes some use of group theory. For convenience I have summarized the basic ideas which I shall need. I hope that this summary will be sufficient for the few students taking the course who have not encountered group theory before.

0.24 Definition. A *group* is a non-empty set G together with a function $G \times G \to G$ (a *binary operation*) written $(g_1, g_2) \mapsto g_1 \cdot g_2$ which has the following properties.

- **It is associative** which means that $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ for all g_1, g_2, $g_3 \in G$.
- **It has an identity** which means that there is a (unique) element $e \in G$ such that $g \cdot e = g = e \cdot g$ for all $g \in G$.
- **Inverses exist** which means that for each element $g \in G$ there is a (unique) element g' such that $g \cdot g' = e = g' \cdot g$.

A group is said to be *abelian* if the binary operation has the following additional property.

- **It is commutative** which means that $g_1 \cdot g_2 = g_2 \cdot g_1$ for all

0.25 Examples. (a) The integers $\mathbb{Z}$, the rationals $\mathbb{Q}$ and the real numbers $\mathbb{R}$ each is an abelian group under addition $(a, b) \mapsto a + b$. The unit is 0 and the inverse of an element a is $-a$.

(b) The integers $\mathbb{Z}$, the rationals $\mathbb{Q}$ and the real numbers $\mathbb{R}$ are not groups under multiplication $(a, b) \mapsto a \times b = ab$. This binary operation is associative and commutative, 1 is the identity but not every element has an inverse: in $\mathbb{Z}$ only the elements ± 1 have an inverse; in $\mathbb{Q}$ and $\mathbb{R}$ every non-zero element a has an inverse a^{-1} but 0 does not have an inverse.

(c) The non-zero rationals $\mathbb{Q}^*$ and the non-zero real numbers $\mathbb{R}^*$ are abelian groups under multiplication.

(d) The binary operation given by subtraction $(a, b) \mapsto a - b$ on the integers $\mathbb{Z}$ is not associative, doesn't have a unit (so that there is no idea of an inverse) and is not commutative.

(e) The set of $n \times n$ non-singular (invertible) matrices is a group, known as the *general linear group* under multiplication. The unit is the identity matrix and the inverse is given by the usual matrix inverse.

(f) The set of congruence classes of integers modulo n, $\mathbb{Z}_n$, is an abelian group under addition (see Eccles, Chapter 21 for this set and the definition of addition).

0.26 Remarks. (a) If a binary operation has a unit then it is necessarily unique for, given units e_1 and e_2, then $e_1 = e_1 \cdot e_2$ (since e_2 is a unit) $= e_2$ (since e_1 is a unit).

(b) Given a set G with binary operation with a unit, if an element $g \in G$ has in inverse then it is necessarily unique since, given inverses g' and g'', $g' = g' \cdot e = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = e \cdot g'' = g''$.

(c) Associativity means that we can write compositions of more than elements without brackets: in a group the expression $g_1 \cdot g_2 \cdot g_3$ is unambiguous since $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

(d) Notations like $(g_1, g_2) \mapsto g_1 \cdot g_2$ or $g_1 * g_2$ are usually used initially when discussing a general binary operation. In practice when discussing groups the binary operation is often called the product or multiplication (represented by $(g_1, G_2) \mapsto g_1 \times g_2$ or just $g_1 g_2$ with the identity either denoted either e or 1 and the inverse of g denoted g^{-1}) or if the group is abelian it is called the sum or addition (represented by $(g_1, g_2) \mapsto g_1 + g_2$ with identity denoted either e or 0 and the inverse of g denoted $-g$). The notes for the course use the product notation.

0.27 Definition. A function $f\colon G_1 \to G_2$ between two groups is called a *homomorphism* if $f(g_1 g_2) = f(g_1) f(g_2)$ for each $g_1,\ g_2 \in G$.

An injection $f\colon G_1 \to G_2$ which is a homomorphism is called a *monomorphism*.

A surjection $f\colon G_1 \to G_2$ which is a homomorphism is called an *epimorphism*.

A bijection $f\colon G_1 \to G_2$ which is a homomorphism is called an *isomorphism*. If there is an isomorphism between two groups G and G_2 then we say that they are isomorphic and write $G_1 \cong G_2$.

0.28 Proposition. (a) If $f\colon G_1 \to G_2$ is a homomorphism of groups then, if e_1 is the identity element of G_1, $f(e_1)$ is the identity element of G_2 and,

for $g \in G_1$, $f(g^{-1})$ is the inverse of $f(g)$ in G_2.

(b) Given homomorphisms of groups $f_1 \colon G_1 \to G_2$ and $f_2 \colon G_2 \to G_3$, then the composition $f_2 \circ f_1 \colon G_1 \to G_3$ is a homomorphism.

(c) If $f \colon G_1 \to G_2$ is an isomorphism of groups then the inverse map $f^{-1} \colon G_2 \to G_1$ is a homomorphism (and so an isomorphism).

Proof. (a) Write e_i for the unit of G_i $(i = 1, 2)$. Since $e_1 e_1 = e_1$ it follows that $f(e_1)f(e_1) = f(e_1)$. Hence $f(e_1) = f(e_1)e_2 = f(e_1)f(e_1)f(e_1)^{-1} = f(e_1)f(e_1)^{-1} = e_2$.
For $g \in G$, $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_1) = e_2$ and, similarly, $f(g^{-1})f(g) = e_2$ so that $f(g^{-1}) = f(g)^{-1}$.

(b) For $g_1, g_2 \in G$, $(f_2 \circ f_1)(g_1 g_2) = f_2\big(f_1(g_1 g_2)\big) = f_2\big(f_1(g_1)f_1(g_2)\big)$ (since f_1 is a homomorphism) $= f_2\big(f_1(g_1)\big)f_2\big(f_1(g_2)\big)$ (since f_2 is a homomorphism) $= (f_2 \circ f_1)(g_1)(f_2 \circ f_1)(g_2)$. Hence $f_2 \circ f_1$ is a homomorphism.

(c) Given $h_1, h_2 \in G_2$, since f is a bijection $h_i = f(g_i)$ for a unique $g_i \in G_1$ $(i = 1, 2)$. Then $f^{-1}(h_i) = g_i$. Since $f(g_1 g_2) = f(g_1)f(g_2) = h_1 h_2$ and f is a bijection, $f^{-1}(h_1)f^{-1}(h_2) = g_1 g_2 = f^{-1}(h_1 h_2)$ as required to prove that f^{-1} is a homomorphism. Since it is also a bijection (the inverse of a bijection) it is an isomorphism. □

0.29 Definition. Given a group G a subset $H \subset G$ is a *subgroup* of G if it is a group under the restriction of the binary operation on G to H.

0.30 Examples. (a) The additive group of the integers $\mathbb{Z}$ is a subgroup of the additive group of the rationals $\mathbb{Q}$.

(b) The even integers form a subgroup of the additive group of the integers.

(c) The singleton subset of G consisting of the identity $\{e\}$ is a subgroup of G called the *trivial subgroup*. This subgroup is denoted by I.

0.31 Definition. Given a homomorphism of groups $f \colon G_1 \to G_2$, the *kernel* of f is defined by $\ker(f) = \{\, g \in G_1 \mid f(g) = e \,\}$ where e is the identity element of G_2.

0.32 Proposition. (a) The kernel $\ker(f)$ of a group homomorphism $f \colon G_1 \to G_2$ is a subgroup of G_1.

(b) A group homomorphism $f \colon G_1 \to G_2$ is a monomorphism if and only if

$\ker(f) = I$, the trivial subgroup of G_1.

Proof. (a) This is a simple check. [In what follows the identity elements of G_1 and G_2 are each denoted e as is usual. It is clear from the context which identity element is meant.] Given g_1, $g_2 \in \ker(f)$, $f(g_1g_2) = f(g_1)f(g_2) = ee = e$ and so $g_1g_2 \in \ker(f)$. Since $f(e) = e$, it follows that $e \in \ker(f)$ and, for $g \in \ker(f)$, $f(g^{-1}) = f(g)^{-1} = e^{-1} = e$ and so the inverse $g^{-1} \in \ker(f)$. Hence $\ker(f)$ is a subgroup of G_1.

(b) Since $f(e) = e$, if f is a monomorphism and so an injection then $\ker(f) = \{e\} = I$. Conversely, if $\ker(f) = I$, then given g_1, $g_2 \in G_1$ such that $f(g_1) = f(g_2)$ it follows that $f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_2)f(g_2)^{-1} = e$ and so $g_1g_2^{-1} \in \ker(f)$ which means that $g_1g_2^{-1} = e$ giving $g_1 = g_2$ proving that f is an injection and so a monomorphism. □

0.33 Proposition. Given groups G and H, a group structure may be put onto the cartesian product $G \times H$ by $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$.

Proof. It is straightforward to check the conditions. The identity is given by (e, e) and the inverse of (g, h) is given by (g^{-1}, h^{-1}). □

References

- P.J. Eccles, *An Introduction to Mathematical Reasoning: numbers, sets and functions,* Cambridge University Press, 1997, chapter 21.