10. Groups

Definition. A group is a set G with binary operation $*$ satisfying the following axioms:

(G0) G is closed under $*$, that is, $(x \in G, y \in G \Rightarrow x * y \in G)$

(G1) $*$ is associative, that is, $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$

(G2) (existence of identity element): there exists $e \in G$, called *identity element* such that $x * e = e * x = x$ for all $x \in G$.

(G3) (existence of inverses): for every $x \in G$ there exists $y \in G$, called *inverse of* x, such that $x * y = y * x = e$. We will usually denote the inverse of x by x^{-1}, but there are some important exceptions where such notation could be confusing (see Example 1 below).

Remark:

(1) Technically, the axiom (G0) does not have to be mentioned explicitly, as it is implied by the assumption that $*$ is a binary operation on G. However, it is useful to keep it in the list, as it is one of the properties (in some cases the only non-trivial property) that needs to be verified when we are trying to show that something is a group.

(2) The axioms of a group do not explicitly require that the identity element e is unique or that every x has unique inverse. However, it turns out that the uniqueness statement is true in both cases and will be proved in the next lecture (as a consequence of the axioms).

(3) The group operation $*$ is not required to be commutative, so it is perfectly fine to have $x * y \neq y * x$ for some $x, y \in G$. However, some pairs of elements of G will always commute; for instance $x * e = e * x$ for every $x \in G$ by (G2).

10.1. Examples (and some non-examples) of groups.

Example 1. *Let R be any ring (not necessarily commutative). Then $(R, +)$ is a group, that is, if we let $G = R$ and define the operation $*$ on G by $x * y = x + y$ for all $x, y \in G$, then G is a group with respect to this operation.*

Let us verify the axioms. In this case we do not need to do any calculations, but simply refer to the suitable axioms of a ring. Indeed, (G0) is precisely the axiom (A0) of a ring (which says that R must be closed under $+$).

(G1) is precisely ring axiom (A2)

(G2) holds if we set $e = 0$. Indeed, $x * e = x + 0 = x = 0 + x = e * x$ for all $x \in R$ by the ring axiom (A3)

Finally, (G3) holds if we set $y = -x$, the additive inverse. Indeed, $x + (-x) = (-x) + x = 0$ by the ring axiom (A4).

Remark:

(1) In Example 1 we do NOT want to denote the group inverse $-x$ by x^{-1} since x^{-1} already has a different meaning, namely the (multiplicative) inverse of x in the ring R (which may or may not exist, depending on x). Thus, if we use the notation x^{-1} for the inverse in the group, it will not be clear which inverse we are talking about.

(2) Since addition is commutative by axiom (A1), in Example 1 we do have property $x * y = x * x$ for all $x, y \in G$ (which, as we already emphasized, does not have to hold in groups in general). Groups satisfying this additional property are called *abelian* (or *commutative*).

(3) Example 1 is really not a single example, but a whole family of examples. As special cases, we obtain the following examples of groups: $(\mathbb{Z}, +)$ (integers with addition), $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}_n, +)$ for every $n \in \mathbb{N}$, $(2\mathbb{Z}, +)$.

Example 2. *Let F be any field. Then $(F \setminus \{0\}, \cdot)$ is a group, that is, $G = F \setminus \{0\}$ (the set of all nonzero elements of F) is a group with respect to multiplication ($* = \cdot$).*

Verification of axioms in this example is similar to Example 1, but a bit more subtle. Let us start with (G0). Note that $(M0)$ states that F is closed with respect to multiplication, but this is not enough for (G0) – we need to check that if $x \in F \setminus \{0\}$ and $y \in F \setminus \{0\}$, then $xy \in F \setminus \{0\}$ or, equivalently, $(x, y \in F, x \neq 0, y \neq 0 \Rightarrow xy \neq 0)$. We know that the latter property is true by a Homework#1 problem, so (G0) is satisfied.

(G1) is precisely the field axiom (M1)

(G2) holds if we set $e = 1$ – this holds by the field axiom (M3)

Finally, (G3) holds if we set $y = x^{-1}$ (the multiplicative inverse of x) – this follows primarily from the field axiom (M4), but (similarly to verification of (G0) above) there is an additional thing to check. Indeed, (M4) says that for every $x \in F \setminus \{0\}$ there exists $y \in F$ such that $xy = yx = 1$. To deduce (G3) we need to check that this y is nonzero (to make sure y is also an element of $G = F \setminus \{0\}$). But this is easy to prove by contradiction: if $y = 0$

and $xy = xy = 1$, then by Lecture 1 we have $0 = x \cdot 0 = 1$, contrary to the axiom $0 \neq 1$.

Example 3. *(generalization of Example 2). Let R be a ring with 1, and let $R^\times$ denote the set of invertible elements of R. Then $(R^\times, \cdot)$ is a group.*

Verification of axioms in this example is similar to Example 2. The only difference is that we have to explicitly check axiom (G0) instead of referring to a previously established property. In this case (G0) asserts that the product of two invertible elements of R is itself an invertible element of R. Verification of this property will be included in Homework#5.

Note that Example 3 is indeed a special case of Example 2 since if R is a field, then $R^\times = R \setminus \{0\}$ by field axiom (M4).

We proceed with two non-examples of groups.

Example 4. *Let O denote the set of all ODD integers. Then $(O, +)$ is not a group.*

Already the first axiom (G0) fails here: since the sum of two odd integers is even, O is not closed under addition. It is also easy to check that (G2) fails (and (G3) does not even make sense without (G2)); however, we do not have mention this explicitly. To prove that something is not a group we just need to exhibit one axiom which does not hold.

Example 5. *Again let O be the set of all odd integers. Then $(O, \cdot)$ is not a group.*

In this example it is easy to see that (G0), (G1) and (G2) hold, with $e = 1$ in (G2). However, (G3) does not hold – for instance there is no $y \in O$ such that $3y = 1$.

Example 6. *(symmetric groups) Let A be any set and let G be the set of all bijective functions $f : A \to A$. Given $f, g \in G$, define $f * g = f \circ g$, the composition of f and g, that is, $(f * g)(a) = f(g(a))$ for all $a \in A$. Then $(G, *)$ is a group. This group is usually denoted by $Sym(A)$ and called the symmetric group on A.*

Verification of axioms in this example boils down to basic properties of composition of functions and will be omitted. We will just state what is the identity element in this group and what are the inverses.

Clearly, (G2) holds if we set $e = id$, the identity function, defined by $id(a) = a$ for all $a \in A$ (the function which sends every element of A to itself). The inverse of $f \in G$ is the inverse function f^{-1} (in the usual sense). Note that $f^{-1} : A \to A$ exists precisely because f is bijective.

Example 7. *(octic group) Let S denote a square centered at $(0,0)$ with sides parallel to coordinate axes. Let G denotes the set of all isometries of S, that is, the set of all bijective functions from S to S which preserve distances between points. A theorem from geometry asserts that G has 8 elements:*

$$G = \{r_0, r_1, r_2, r_3, s_1, s_2, s_3, s_4\}$$

where r_k is the counterclockwise rotation by $90k$ degrees for $k = 0, 1, 2, 3$, and s_1, s_2, s_3 and s_4 are reflections with respect to the lines $y = 0$, $y = x$, $x = 0$ and $y = -x$, respectively.

Then G is a group with respect to composition. In the sequel this group will be denoted by D_8 and called the dihedral group of order 8 (later we will consider the groups D_{2n} for every integer $n \geq 3$).

As in Example 6 we will skip verification of axioms and state what is the identity in G and compute the inverses. Clearly, r_0 is the identity element of G, and inverses are as follows: $r_1^{-1} = r_3$, $r_3^{-1} = r_1$, and every other element of G is its own inverse: $x^{-1} = x$ for all $x \neq r_1, r_3$.

Example 8. *(general linear group) Let F be a field, let $n \geq 2$ be an integer, and let $GL_n(F)$ be the set of all invertible $n \times n$ matrices with entries in F, that is,*

$$GL_n(F) = \{A \in Mat_n(F) : \text{ there exists } B \in Mat_n(F) \text{ s.t. } AB = BA = I\}$$

where I is the identity matrix. Then $GL_n(F)$ is a group with respect to matrix multiplication.

There are two different ways to check that $GL_n(F)$ is group.

The first way, which is shorter but more abstract, is to observe that the set $Mat_n(F)$ of all $n \times n$ matrices over F is a ring (with respect to matrix addition and multiplication) and by definition $GL_n(F) = (Mat_n(F))^\times$, the set of invertible elements of $Mat_n(F)$. Hence by the result of Example 3, $GL_n(F)$ is a group with respect to matrix multiplication.

The identity element of $GL_n(F)$ is the identity matrix I, and the inverse of $A \in GL_n(F)$ is the inverse matrix in the usual sense.

The second argument is more explicit and uses the following fact from linear algebra: a matrix $A \in Mat_n(F)$ is invertible if and only if $\det(A) \neq 0$. Thus, $GL_n(F) = \{A \in Mat_n(F) : \det(A) \neq 0\}$. Using this alternative description, one can now verify group axioms similarly to Example 3. In order to check (G0) with this approach we need to use the following basic property of determinants: that $\det(AB) = \det(A) \cdot \det(B)$.