11. General results about groups

Recall that in the last lecture we defined groups and introduced several (classes of) examples of groups. We start this lecture by establishing some general properties that hold in all groups (similarly to what we did with rings in Lecture 1).

Theorem 11.1. *Let $(G, *)$ be a group. The following hold:*

(a) *Identity element $e \in G$ is unique.*
(b) *For every $x \in G$, its inverse x^{-1} is unique.*
(c) *(cancellation laws) If $a * x = a * y$ for some $a, x, y \in G$, then $x = y$. Similarly if $x * a = y * a$ for some $a, x, y \in G$, then $x = y$.*
(d) *If $a * z = e$ for some $a, z \in G$, then $a = z^{-1}$ (and $z = a^{-1}$).*
(e) *$(x * y)^{-1} = y^{-1} * x^{-1}$ for all $x, y \in G$.*

Proof. To be included. □

Multiplicative notation in groups. From now on, given a group G and $x, y \in G$, we will usually write xy instead of $x * y$ (this is what we call multiplicative notation) and refer to group operation as *multiplication*.

We will NOT be using multiplicative notation when the multiplication symbol already has some meaning in G, and its meaning is different from group operation (so the use of multiplicative notation may be confusing). For instance, suppose that $G = (\mathbb{Z}, +)$, that is $G = \mathbb{Z}$ as a set, and the group operation is addition. In this case we do NOT write xy instead of $x + y$ to avoid confusion with the (usual) multiplication in $\mathbb{Z}$.

Once we start using multiplicative notation in groups, it is tempting to start applying the same rules that we routinely use when working with products of, say, real numbers. Some of the usual rules will still hold in arbitrary groups, while some will not. For instance,

(i) We do not have to write parentheses since $(xy)z = x(yz)$ by associativity (G1), so we can simply write xyz.
(ii) On the other hand, we cannot change the order of factors: $xy \neq yx$ in groups in general since we do not assume that group operation is commutative.

The multiplication table of a group. Let G be a group with operation $*$. The *multiplication table of G* is a table whose rows and columns are labeled by elements of G, and at the intersection of x-row and y-column we put element $x * y$. Let us consider two examples.

1. Let $G = (\mathbb{Z}_5, +)$. Since the group operation in this example is addition, the multiplication table of G is the same as the addition table of the ring $\mathbb{Z}_5$:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

2. Let $G = (\mathbb{Z}_5 \setminus \{[0]\}, \cdot)$, the set of nonzero elements of $\mathbb{Z}_5$ with group operation given by multiplication in $\mathbb{Z}_5$. In this case the multiplication table for G is the same as the multiplication table for the ring $\mathbb{Z}_5$ with row and column labeled by 0 removed (since 0 is not an element of G).

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Looking at multiplication tables in these two examples, we immediately observe two properties:

(i) The tables are symmetric with respect to the main diagonal. This holds precisely because both of those groups are commutative ($x*y = y*x$ for $x, y \in G$). Since commutativity is not required in groups, this property will not hold for group multiplication tables in general.

(ii) The "Sudoku property": every row and column contains every element of the group precisely once. This property WILL hold in arbitrary groups and follows easily from the cancellation laws (part (c) of Theorem 11.1). Formal verification of this property is left as a homework exercise.