Graduate Algebra, Fall 2014
Lecture 1

Andrei Jorza

2014-08-27

1 Group Theory

1.1 Basic definitions

Let G be a set and $\cdot$ be a binary operation on G. Say that:

1. $\cdot$ is **associative** if for any $x, y, z \in G$ have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. With induction you can also show that for all $x_1, \ldots, x_n \in G$ the value of $x_1 \cdot x_2 \cdots x_n$ is independent of the order in which the $\cdot$ operations are performed.
2. $\cdot$ has a unit element e if for all $x \in G$ one has $x \cdot e = e \cdot x = x$. Unit elements, if they exist, are unique: indeed, if e, e' are units then $e = e \cdot e' = e'$.
3. an element $x \in G$ has an inverse x^{-1} if $x \cdot x^{-1} = x^{-1} \cdot x = e$. If G is associative then inverses, if they exist, are unique. Suppose a, b are inverses to x. Then $a = ae = a(xb) = (ax)b = eb = b$.
4. $\cdot$ is commutative or abelian if $xy = yx$ for all $x, y \in G$.

We say that G with $\cdot$ is:

1. a **semigroup** if $\cdot$ is associative.
2. a **monoid** if G is a semigroup and there exists a unit.
3. a **group** if G is a monoid and every element has an inverse.

A list of many examples:

1. $\mathbb{Z}$ with $+$ and 0 is a group.
2. $\mathbb{Z}_{\geq 0}$ with $+$ and 0 is a monoid.
3. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with $+$ and 0 are groups.
4. for $n \geq 2$ an integer $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ with addition modulo n and 0 is a group.
5. for $n \geq 2$ an integer $(\mathbb{Z}/n\mathbb{Z})^\times = \{d \in \mathbb{Z}/n\mathbb{Z} | (d, n) = 1\}$ with multiplication modulo n and 1 as unit is a group.
6. $\mathbb{Q}/\mathbb{Z} = [0, 1) \cap \mathbb{Q}$ with unit 0 and addition defined as

$$x``+'' y = x + y \mod 1 = \{x + y\} = \begin{cases} x + y & x + y < 1 \\ x + y - 1 & x + y \geq 1 \end{cases}$$

is a group (here $\{x\}$ represents the fractional part).

7. If $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are two groups then $(G \times H, \cdot, e_G \times e_H)$ is a group where $\cdot$ is defined component-wise. For example the Klein group is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{(0,0), (0,1), (1,0), (1,1)\}$.

8. For $n \geq 2$, S_n is the group of permutations of a fixed set of n elements. Multiplication is composition of permutations and the identity is the identity permutation.

9. The dihedral group D_{2n} is the group of symmetries of a regular n-gon. Again, multiplication is composition of symmetries and the identity map is the identity element.

10. If R is $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ and $n \geq 1$ then the set $M_{n\times n}(R)$ of $n \times n$ matrices with entries in R is a group with respect to matrix addition.

11. If R is $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ then the set $\mathrm{GL}(n, R)$ of $n \times n$ matrices with entries in R and non-zero determinant is a group with respect to matrix multiplication.

1.2 Cyclic groups

The simplest groups are the cyclic ones. An infinite cyclic group is a group G, written multiplicatively, whose elements are $\{1, a^{\pm 1}, a^{\pm 2}, \ldots\}$ where $a \in G$ is such that $a^n \neq 1$ for any $n \in \mathbb{Z}$. The element a is called a **generator** of G (we write $G = \langle a \rangle$) and say that a has infinite order.

A finite cyclic group of order n is a group G, written multiplicatively, whose elements are $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a \in G$ such that $a^n = 1$ but $a^d \neq 1$ for any $0 < d < n$. Again, a is said to be a generator of G ($G = \langle a \rangle$) and we say that a has order $\mathrm{ord}(a) = n$.

If G is any group and $a \in G$ we can still define the order of a as above.

Proposition 1. *Suppose $a \in G$ has order n and $d \geq 1$ is an integer. Then* $\mathrm{ord}(a^d) = n/(d,n)$.

Proof. In class I only did the case when $(d,n) = 1$. Suppose $m = \mathrm{ord}(a^d)$. Then m is the smallest positive integer such that $(a^d)^m = a^{dm} = 1$. Certainly $(a^d)^{n/(d,n)} = (a^n)^{d/(d,n)} = 1$ and so $m \leq n/(d,n)$ by the minimality assumption.

Next, use division with remainder to write $md = qn + r$ where $0 \leq r < n$. This is a phenomenally powerful tool that we'll use many times. Then

$$1 = a^{dm} = a^{qn+r} = (a^n)^q a^r = a^r$$

Since a has order n and $r < n$ it follows that r must be 0. Thus $dm = qn$ and we can rewrite this as

$$\frac{d}{(d,n)} m = \frac{n}{(d,n)} q$$

Now $d/(d,n)$ and $n/(d,n)$ are coprime and so, by unique factorization in the integers, it follows that $n/(d,n) \mid m$. As $m > 0$ this implies that $m \geq n/(d,n)$ and so we deduce, from the above, that $m = n/(d,n)$ as desired. $\square$