Linear Algebra & Geometry

LECTURE 3

Groups

Definition. An algebra (G,*) is called a *group* iff

1. * is associative
$$(\forall p, q, r \in G)\ p * (q * r) = (p * q) * r$$
2. G has an identity element
$$(\exists e \in G)(\forall p \in G)\ e * p = p * e = p$$
3. Every element of G is invertible
$$(\forall p \in \mathrm{G})(\exists q \in G) p * q = q * p = e$$

A group is called *Abelian* if

4. * is commutative
$$(\forall p, q \in G) p * q = q * p$$

Remark. Due to axiom 2 no group is empty.

Fact.
There is only one identity element in a group.
For every element in a group there is only one inverse element.

Proof.
If e and d are identity elements then $e * d = d$ because e is an identity, and $e * d = e$ because d is an identity. There is only element $e * d$ (an algebraic operation is a function) so $e = d$.

Comprehension test.
Prove the uniqueness of the inverse element.

Note.
We tend to denote the inverse element to p by p^{-1}. Be warned – this is a general symbol, nothing to do with $\frac{1}{p}$ in "regular" arithmetic of numbers.

Examples.

- $(\mathbb{Z},+)$, $(\mathbb{R},+)$ are Abelian groups
- Let $X = \{2k + 1 | k \in \mathbb{Z}\}$. $(X, +)$ is not a group for a number of reasons. First and most important (and also most likely to be overlooked) is that it is not an algebra at all, because the sum of two numbers from X does not belong to X.
- Let $X = \{2k | k \in \mathbb{Z}\}$. $(X, +)$ is an Abelian group. First, it is an algebra (it is"*closed under addition*") i.e. the sum of two even numbers is even. Associativity and commutativity or addition are obvious. 0 is the identity and $-a$ is the inverse for a.
- $(\mathbb{R},\cdot)$ is not a group because 0 is not invertible. $(\mathbb{R} \setminus \{0\},\cdot)$ is a group, though.
- $(\mathbb{R}^+,\cdot)$ is a group, ($\mathbb{R}^+ = (0; \infty)$ and $\cdot$ denotes multiplication in the usual sense). $(\mathbb{R}^-,\cdot)$ is not a group because it is not *closed under multiplication*.

- $(2^X, \div)$ where 2^X is the set of all subsets of X and $A \div B = (A \cup B) \setminus (A \cap B)$ is an Abelian group. 2^X is obviously *closed under symmetric difference*. It is easy to verify that the identity element is $\emptyset$ and that for every subset A of X, $A^{-1} = A$.

Comprehension.
Prove that symmetric difference is associative.

Fact.

- $A \div B$ can be equivalently defined as $(A \setminus B) \cup (B \setminus A)$.
- $A \div B$ can be described as the set of all those elements of X who belong to exactly one of A and B.

Operations modulo *n*

Lemma. (Remainder lemma for integers).
For every $k \in \mathbb{Z}$ and for every $n \in \mathbb{N}$ there exist unique q and r such that $k = nq + r$, $q \in \mathbb{Z}$ and $0 \leq r \leq n - 1$.

The number *r* is called the *remainder from the division of k by n* and is often denoted by $k \; mod \; n$ (*k modulo n*). Obviously, for every integer *p*, $k \; mod \; n = (k + pn) mod \; n$

Definition.
For every $n \in \mathbb{N}$ and for every $p, q \in \mathbb{Z}$
$p \oplus q = (p + q) mod \; n$ (*addition modulo n)*

$p \otimes q = (pq) mod \; n$ (*multiplication modulo n*).

Comment. The meaning of $\oplus$ and $\otimes$ depends on *n*. To avoid ambiguities we should use clumsy symbols like $\oplus_n$ and $\otimes_n$. Instead, we usually let the context determine the actual value of *n*.

Theorem.
Multiplication and addition mod n are commutative and associative.

Lemma.
(1) $(a \bmod n) \bmod n = a \bmod n$ (obvious)
(2) $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
(3) $(ab \bmod n) = [(a \bmod n)(b \bmod n)] \bmod n$

The lemma and the theorem will be proved in tutorials.

Comprehension.

For which *n* is $(\mathbb{Z}, \oplus_n)$ a group?

Definition.
$\mathbb{Z}_n = \{0,1,\dots,n-1\}$

Fact.
$(\mathbb{Z}_n,\bigoplus)$ is an Abelian group.

Proof.
Addition mod n is an operation on the set $\mathbb{Z}_n$ because the remainder from the division by *n* is always a number between 0 and *n*-1 (never omit this part!).
Addition mod n is associative and commutative.
The identity element for $\bigoplus$ is clearly 0 and **0 belongs to $\mathbb{Z}_n$**.
What is the inverse for a $k \in \mathbb{Z}_n$? It must be $p \in \mathbb{Z}_n$ such that $p \bigoplus k = 0$. Obviously, it cannot be $(-k)$ because it does not belong to $\mathbb{Z}_n$. On the other hand, we don't want $p + k = 0$, we want $p \bigoplus k = 0$. It means we want $p + k$ divisible by *n*. This means a good choice for the inverse to *k* is *n*-*k*, except in the case *k*=0 where *k* is its own inverse. QED

Examples – continued

- $(\mathbb{Z}_6, \otimes)$ is associative, commutative, 1 is the identity element. But it is not a group because 0 is not invertible: for every *k*, $k \otimes 0 = 0$, never 1. We can try to save the case by removing 0 from $\mathbb{Z}_6$, like we did in case of $\mathbb{R}$. Unfortunately, $(\mathbb{Z}_6 \setminus \{0\}, \otimes)$ is not closed under multiplication, e.g. $2 \otimes 3 = 0$ and $0 \notin \mathbb{Z}_6 \setminus \{0\}$, obviously.
- Let *BI*(*X*) denote the set of all functions from X into X that are injective ("*one-to-one*") and surjective ("*onto*").
  A function $f : X \to Y$ is said to be *injective* iff
  $(\forall p, q \in X)\ (p \neq q \Rightarrow f(p) \neq f(q))$.
  A function $g : X \to Y$ is said to be *surjective* iff
  $$(\forall y \in \mathrm{Y})(\exists x \in X) f(x) = y$$
  The *composition* of functions *f* and *g* is the function $f \circ g$ such that $(\forall x \in X)(f \circ g)(x) = f(g(x))$.

Comprehension.

- Prove that composition is an operation on $BI(X)$.
- Prove that composition is associative.
- Describe all cases when composition is commutative.
- Show that $(BI(X),\circ)$ is a (usually non-Abelian) group.

Fact. (The cancellation law)

In every group $(G,*)$

1. $(\forall a,b,c \in G)(a * c = b * c \Rightarrow a = b)$ (*right cancellation law*)
2. $(\forall p,q,r \in G)(p * q = p * r \Rightarrow q = r)$ (*left cancellation law*)

Proof.

Part 1. $(a * c) * c^{-1} = (b * c) * c^{-1}$ because $a * c = b * c$ and an algebraic operation is a function. Since $*$ is associative we get $a * (c * c^{-1}) = b * (c * c^{-1})$ which yields $a=b$.
Part 2. can be done in the same way.

Fact.

In every group $(G,*)$

1. $(\forall a,b \in G)(a*b)^{-1} = b^{-1}*a^{-1}$
2. $(\forall a \in G)(a^{-1})^{-1} = a$

Proof.

Part 1. How does one verify that p is the inverse for q? We check if $p*q = q*p = e$. Here we want to show that $b^{-1}*a^{-1}$ is the inverse for $a*b$. Let us put $p = b^{-1}*a^{-1}$ and $q = a*b$. We get $(b^{-1}*a^{-1})*(a*b) = ((b^{-1}*a^{-1})*a)*b =$ $(b^{-1}*(a^{-1}*a))*b = (b^{-1}*e)*b = b^{-1}*b = e$. The other equality, $(a*b)*(b^{-1}*a^{-1}) = e$, can be done the same way.

Part 2. We use the same idea. How do we check that the inverse for a^{-1} is a? We just check if $a^{-1}*a = e$ but this is obvious so, in a sense, there is nothing to prove.

Definition.
A group $(H, \#)$ is said to be a *subgroup* of a group $(G, *)$ iff $H \subseteq G$ and $(\forall a, b \in H) a \# b = a * b$.

We usually say that H is a subgroup of G with respect to the same operation and we write $(H, *)$. It would be better to say that the operation on H is the one we use in G only *restricted* to $H \times H$. But then we would have to write $(H, * \mid_{H \times H})$ which looks untidy.

Fact.
If H is a subgroup of G then the identity element in H is the same as the identity of G and the inverse of an element *a* in H is the same as the inverse of *a* in G.

Proof. Suppose e_H is the identity of H which means that $e_H * e_H = e_H$. Since $H \subseteq G$, e_H is an element of G and is therefore invertible in G. Hence, there exists $q \in G$ such that $e_H * q = e$. From $e_H * e_H = e_H$ we get $(e_H * e_H) * q = e_H * q$, which yields $e_H * e = e$ and, finally, $e_H = e$. In a similar way we can show that $(p^{-1})_H = (p^{-1})_G$. QED

Examples.

1. $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ (the set of all even integers) is a subgroup of $\mathbb{Z}$ (with resp. to regular addition).
2. The set of odd integers is not a subgroup of $\mathbb{Z}$.
3. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{Q}(\sqrt{2}), +)$, which in turn is a subgroup of $(\mathbb{R}, +)$.
4. $(\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.
   The only nontrivial questions here are:
   (a) is $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ *closed under addition* and
   (b) does the inverse of every number from $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ belong to $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$.
   Proof. (a): $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ which does belong to $\mathbb{Q}(\sqrt{2})$ but does it belong to $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$? Yes, because the product of two non-zero real numbers is a nonzero real number.

(b): $\left(a+b\sqrt{2}\right)^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{(a^2-2b^2)} \in \mathbb{Q}\left(\sqrt{2}\right)$ and, since the inverse to a real number is always non-zero, we can claim that $\left(a+b\sqrt{2}\right)^{-1} \in \mathbb{Q}\left(\sqrt{2}\right) \setminus \{0\}$.

Note. You have probably noticed that the way we define $\mathbb{Q}\left(\sqrt{2}\right)$ over $\mathbb{Q}$ mimics the way we defined complex numbers over reals. We could say $\mathbb{C} = \mathbb{R}(i)$.

Comprehension.

1. Is $(\mathbb{Z}_6, \oplus)$ a subgroup of $(\mathbb{Z}, +)$?
2. Consider $(BI(\mathbb{R} \times \mathbb{R}), \circ)$ – the group of all bijections of the plane onto itself. Is the set of all bijections that preserve the distance between points a subgroup? (f *preserves the distance* iff $(\forall P, Q \in \mathbb{R}^2) dist(P, Q) = dist(f(P), f(Q))$).