OLGA RADKO MATH CIRCLE, SPRING 2024: ADVANCED 3

FERNANDO FIGUEROA AND JOAQUÍN MORAGA

Worksheet 5: Abelian Groups

A set G with a binary operation [1] $\cdot_G$ is said to be a group $(G, \cdot_G)$ if it satisfies the following properties:

(1) Associativity: For any a, b, c in G, we have the following equality:
$$(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$$
(2) Identity element: There exists a unique element e in G, such that for any a in G:
$$a \cdot_G e = e \cdot_G a = a$$
(3) Inverse element: For any element a in G, there exists an inverse element represented as a^{-1}, such that:
$$a \cdot_G a^{-1} = a^{-1} \cdot_G a = e$$

If furthermore the operation is commmutative, we say that the group is abelian.

Problem 5.1:

(1) Show that $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group.
(2) Show that $(\mathbb{Z}, +)$ is a group.

Solution 5.1:

[1] binary operations take two elements g and h and give an element $g \cdot_G h$, for example the usual addition an product are binary operations.

Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the set of positive integers less than n that are coprime with n.

Problem 5.2:

(1) Show that $(\mathbb{Z}/n\mathbb{Z})^\times$ with multiplication defined in $\mathbb{Z}/n\mathbb{Z}$, is an abelian group.
(2) Is $(\mathbb{Z}/n\mathbb{Z})^\times$ with addition defined in $\mathbb{Z}/n\mathbb{Z}$, an abelian group?

Solution 5.2:

Let $\mathbb{F}$ be a field.

Problem 5.3:

(1) Show that $(\mathbb{F}, +)$ is an abelian group
(2) Show that the nonzero elements of $\mathbb{F}$, together with the product defined in the field is an abelian group.

Solution 5.3:

We will sometimes use additive notation $(G, +)$, and we will write $-a$ for the inverse of a, and the identity element will be called 0. Other times we will use multiplicative notation $(G, \cdot)$ and we will write a^{-1} for the inverse of a, and the identity element will be called 1.

An element P of a group $(E, +_E)$ is said to have order d if d is the smallest positive integer such that

$$dP = \underbrace{P +_E \cdots +_E P}_{d \text{ times}} = e$$

In multiplicative notation: An element P of a group $(E, \cdot_E)$ is said to have order d if d is the smallest positive integer such that

$$P^d = \underbrace{P \cdot_E \cdots \cdot_E P}_{d \text{ times}} = 1$$

Problem 5.4:

What are the orders of the following elements

(1) 1 in $((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)$
(2) 3 in $((\mathbb{Z}/8\mathbb{Z})^\times, \cdot)$
(3) 5 in $((\mathbb{Z}/24\mathbb{Z})^\times, \cdot)$

Solution 5.4:

Problem 5.5:

Show that if an element a in $(G, \cdot)$ satisfies $a^c = 1$, for some positive integer c, then the order of a divides c.

Solution 5.5:

Let p and q be different prime numbers.

Problem 5.6:

(1) Show that in $((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot)$ the order of every element divides $p-1$
(2) Show that in $((\mathbb{Z}/pq\mathbb{Z})^{\times}, \cdot)$ the order of every element divides $(p-1)(q-1)$
(3) Show that in $((\mathbb{Z}/pq\mathbb{Z})^{\times}, \cdot)$ the order of every element divides $\mathrm{lcm}(p-1)(q-1)$.

Solution 5.6:

A group $(G, +)$ is said to be cyclic if there exists an element A in G, such that any element in G is of the form dA, where d is an integer.

Problem 5.7:

(1) Write the definition of being a cyclic group in multiplicative notation
(2) Show that $((\mathbb{Z}/7\mathbb{Z})^{\times}, \cdot)$ is cyclic.
(3) Show that $((\mathbb{Z}/35\mathbb{Z})^{\times}, \cdot)$ is not cyclic.

Solution 5.7:

Problem 5.8:

(1) Show that a finite group with r elements is cyclic if and only if there exists an element of order r.
(2) Let p and q be two different odd prime numbers. Show that $((\mathbb{Z}/pq\mathbb{Z})^\times, \cdot)$ is not cyclic.

Solution 5.8:

Let $\mathbb{F}$ be a field of characteristic different to 2 or 3.

Let $x^3 + ax + b$ be a cubic polynomial with coefficients in $\mathbb{F}$ that has no repeated roots. An *elliptic curve* over $\mathbb{F}$ is defined as the set of points (x, y) in $\mathbb{F}^2$ satisfying the equation

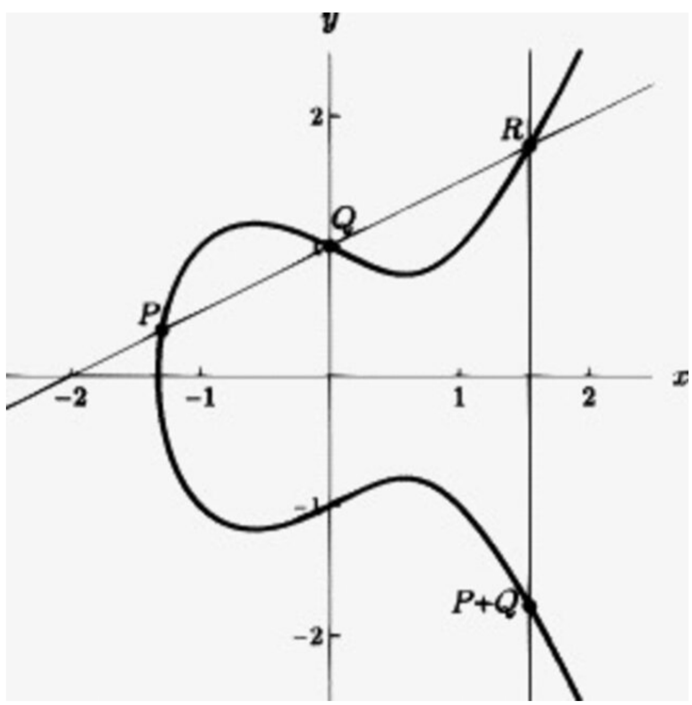
$$y^2 = x^3 + ax + b.$$

Together with a single point denoted O and called the point at infinity.

Let E be an elliptic curve over $\mathbb{R}$, let P and Q be two points in E. We will define $P + Q$ and $-P$ by the following rules.

(1) If $P = O$, then $-P := O$ and $P + Q := Q$, so in the following cases we will assume that no point is the point at infinity.
(2) If the point P has coordinates (x, y), then the point $-P$ is given by the the coordinates $(x, -y)$
(3) If P and Q have different coordinates, then the line $l = \overline{PQ}$ intersects E at a third point R (in case l is tangent to E, we define R to be the point of tangency). We define $P + Q = -R$.
(4) If $Q = -P$, then $P + Q := O$.
(5) If $P = Q$, then let l be the tangent line to E at P, let R be the third point of intersection of l and E. We define $P + Q := -R$.

An example can be seen in the following picture:



The x-coordinates of the point $P+Q$ and $2P$ can be determined by the following formulas:

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

$$x_4 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$$

Where $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P+Q = (x_3, y_3)$ and $2P = (x_4, y_4)$. The elliptic curve has equation $y^2 = x^3 + ax + b$.

The addition of an elliptic curve over an arbitrary field can be defined by using these formulas, or by the definitions given in the previous page, whenever they make sense.

Problem 5.9:

Consider the elliptic curve $y^2 = x^3 - 1$ over $\mathbb{F}_5$.

How many points of each order are there in this elliptic curve?

Solution 5.9:

In the case of elliptic curves over the complex plane, there is a different way to obtain this group.

Given two vectors in $\mathbb{R}^2$ $v_1 = (a_1, b_1)$ and $v_2 = (a_2, b_2)$, such that $(0, 0), v_1, v_2$ are not colinear. We can define the parallelogram given by all the points of the form

$$\alpha v_1 + \beta v_2,$$

where α, β lie in $[0, 1)$. This will be our set E.

Any vector in $\mathbb{R}^2$ can be written uniquely as $xv_1 + yv_2$. If we have two vectors c_1, c_2, then we have $c_1 + c_2 = xv_1 + yv_2$ for some values of x, y in $\mathbb{R}$.

The addition of E is defined by

$$c_1 +_E c_2 := \{x\}v_1 + \{y\}v_2.$$

Where $\{x\}$ denotes the fractional part of a real number.

Problem 5.10:

Show that if one takes $v_1 = (1, 0)$ and $v_2 = (0, 1)$. Then this operation defines an abelian group $(E, +_E)$. Is this true for any v_1 and v_2?

What are the points that satisfy $2P = (0, 0)$?

Solution 5.10:

Problem 5.11:

(1) How many elements of $(E, +_E)$ have order 2?
(2) How many elements of $(E, +_E)$ have order d?

Solution 5.11:

Let $(G, +)$ be an abelian group, a and b elements in G, such that a is of order p and b is of order q.

Problem 5.12:

(1) Show that ab is of order pq, if p and q are different prime numbers
(2) Show that ab is of order pq, if p and q are coprime numbers.

Solution 5.12:

Problem 5.13:

Show that the group structure on the elliptic curve $y^2 = x^3 + 2$ over $\mathbb{F}_7$ is not a cyclic group.

Solution 5.13:

Problem 5.14:

Show that the group structure on the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$ is a cyclic group.

Solution 5.14:

Problem 5.15:

Show that the group structure on an elliptic curve over $\mathbb{R}$ is not a cyclic group.

Solution 5.15:

UCLA Mathematics Department, Los Angeles, CA 90095-1555, USA.
Email address: fzamora@math.princeton.edu

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA.
Email address: jmoraga@math.ucla.edu