Algebra MATH-310

Lecture 4

Anna Lachowska

October ~~6~~ 7, 2024

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Groups: lecture 3

(a) Groups in cryptography: Elliptic curves and Lenstra's factorization algorithm

(b) Non-abelian groups: the dihedral group

(c) Normal subgroups and quotients

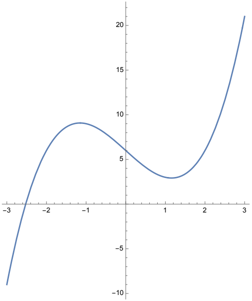
(d) Examples of quotient groups

Elliptic curve group

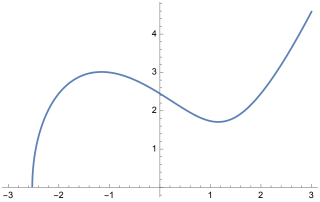
Definition

An elliptic curve is a subset of points in a plane $\mathbb{K}^2$ that satisfy the equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{K}$.

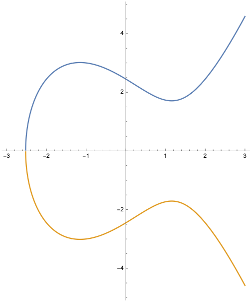
$y = x^3 - 4x + 6$



$y = \sqrt{x^3 - 4x + 6}$



$y^2 = x^3 - 4x + 6$

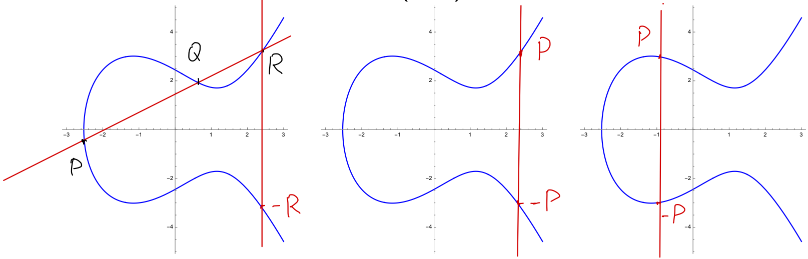


The set of $\mathbb{K}$-rational points on an elliptic curve has a group structure

Set $P+Q=-R$ whenever three points P, Q, R are collinear points on the curve. $P+Q=-R$, $P+R=-Q$, $R+Q=-P$

1. The neutral element is the point O "up at ∞"
2. For any P the opposite point is the point symmetric to P with respect to the horizontal axis. Then $P+(-P)=O$.
3. For any P, we have $P+O$ (vertical line through P) intersects the curve in $-P$, so we have $P+O=-(-P)=P$.

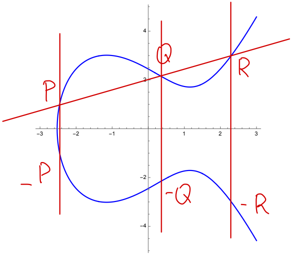
$P+Q=-R$ $\qquad$ $P+(-P)=O$ $\qquad$ $P+O=P$



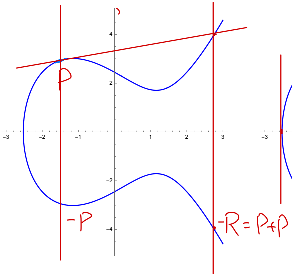
Elliptic curve group

4. If P, Q, R are three intersection points of a line with the curve, then $P + Q = -R$, $Q + R = -P$ and $P + R = -Q$.
5. To find $P + P$, draw a tangent to the curve at P which intersects the curve at R. Then $P + P = -R$, and $P + R = -P$.
6. If P has y-coordinate zero, then $P + P = O$.

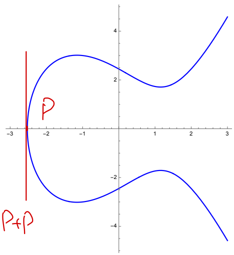
$P + Q = -R$



$P + P = -R$

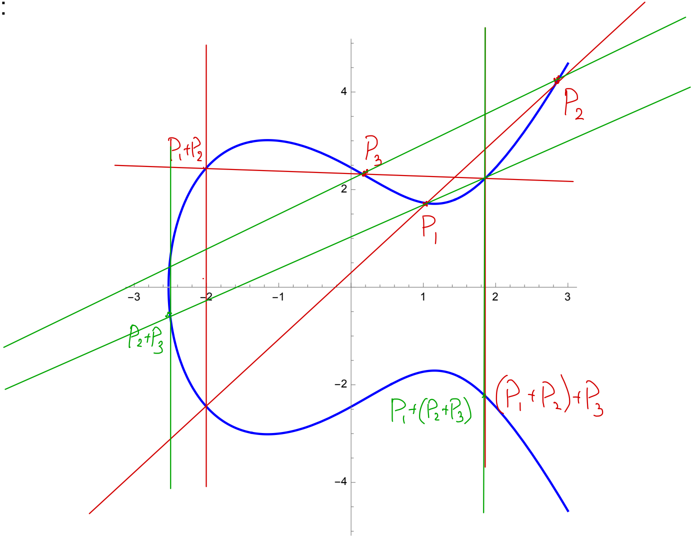


$P + P = O$



Elliptic curve group $(P_1+P_2)+P_3 = P_1+(P_2+P_3)$

The addition is clearly commutative. It is also associative (harder to show).
Example:



Elliptic curve group: conclusions

1. Computing sums and multiples of points involves computing slopes of lines of the form $\frac{u}{v}$.
2. If we consider the curve over numbers $\mathbb{Z}/n\mathbb{Z}$, then the construction fails if and only if v is not invertible modulo n. This is exactly when $\gcd(v, n) > 1$. This is the idea of Lenstra's factorization algorithm (Hendrik Lenstra, 1987).

collaborated with
Arjen Lenstra
(EPFL)

Lenstra's factorization algorithm

Suppose you want to factorize a number $n \in \mathbb{N}$.

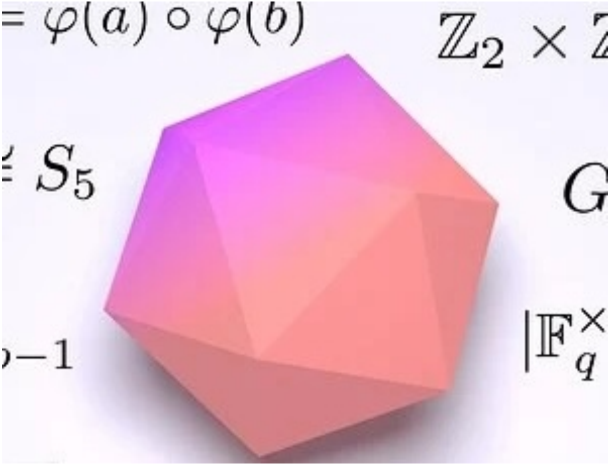
1. Pick up an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}/n\mathbb{Z}$ and a point P on it.
2. Compute $2P$, $3!P$, $4!P$, etc until the computation fails.

   $$3!P = 3 \cdot 2P = 2 \cdot 2P + 2P, \dots$$

   This involves computing slopes of lines $\frac{u}{v}$ modulo n, which makes sense if and only if $\gcd(v, n) = 1$ and v is invertible in $\mathbb{Z}/n\mathbb{Z}$.
3. If the computation fails, this implies $\gcd(v, n) > 1$ and you have found a nontrivial factor of n.
4. Otherwise restart with a different curve and point P.

This method is especially efficient to find small factors of n.

Back to group theory!



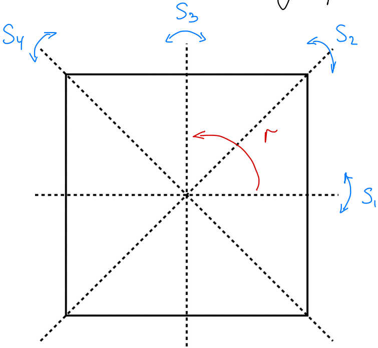
Dihedral group

Definition

D_n, $n \geq 3$, is the group of rigid symmetries of a flat regular n-gon.

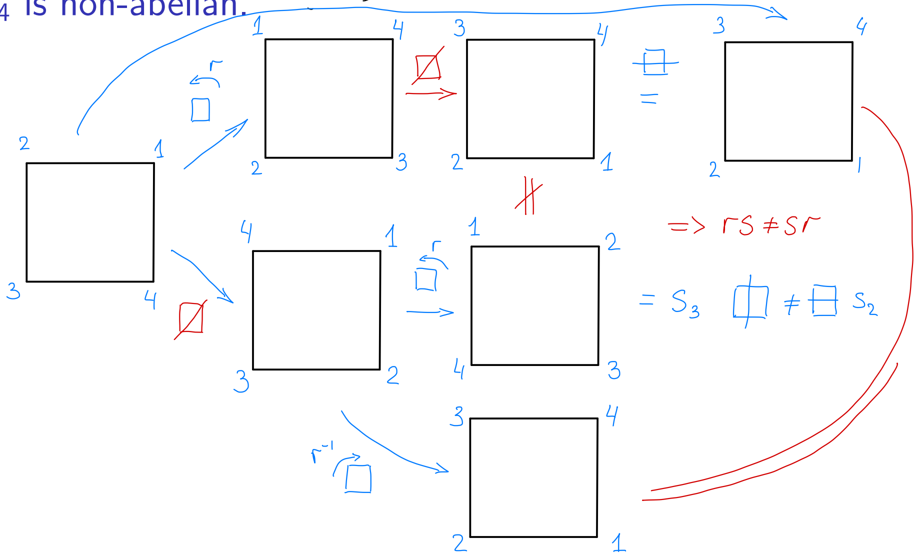
$$D_n = \{1, r, \dots r^{n-1}, s_1, s_2, \dots s_n\}.$$

Example: D_4. $= \{1, r, r^2, r^3, s_1, s_2, s_3, s_4\}$ – a group with respect to compositions



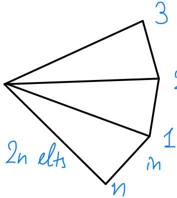
D_4 is non-abelian.

(Also any D_n, $n \geq 3$ is non-abelian)



$\Rightarrow sr = r^{-1}s$ a relation in D_4

Number of elements and relations in D_n:



Vertex 1 $\longrightarrow$ n possibilities

Vertex 2 $\longrightarrow$ 2 possibilities

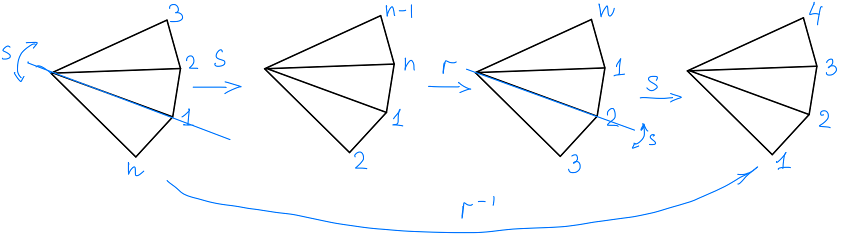
But we have already found $2n$ elts in D_n

$\Rightarrow |D_n| \le 2n$

$\Rightarrow |D_n| = 2n$

Relations in D_n

Let s be a reflection through a vertex, r a counterclockwise rotation by $\frac{2\pi}{n}$.



Conclusion: $srs = r^{-1}$. $\Rightarrow sr = r^{-1}s$, $srsr = 1 \Rightarrow (sr)^2 = 1$

Presentation of D_n in generators and relations

Proposition

D_n admits a presentation in generators and relations:

$$D_n = \langle s, r \mid s^2 = 1, r^n = 1, srs = r^{-1} \rangle.$$

Complete list of elements: $\{\underbrace{1, r, r^2 \dots r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, sr^2 \dots sr^{n-1}}_{\text{reflections}}\}$

Idea: $sr = r^{-1}s \Rightarrow$ Any product $sr^3sr^{-2}s \dots$ can be written in the form $s^a r^b$, $s^2 = 1 \Rightarrow \{r^i, sr^j\}_{\substack{i=0\dots n-1 \\ j=0\dots n-1}} \Rightarrow$ get $2n$ elements

Any additional relation would reduce # of elements in the group.

What do we need it for?

Recall: A subgroup $H \subset G$ is normal in G if $ghg^{-1} \in H$ for any $g \in G$, $h \in H$. If G is abelian, then any subgroup $H \subset G$ is normal: $ghg^{-1} = gg^{-1}h = h \in H$.

If G is non-abelian, the situation is more interesting.

Examples of subgroups in D_n

$$D_n = \langle s, r \mid s^2 = 1, r^n = 1, srs = r^{-1} \rangle.$$

1. Let $R = \langle r \rangle = \{1, r, \dots r^{n-1}\} \subset D_n$ be the subgroup of rotations. Then $R \trianglelefteq D_n$ is normal in D_n:

Need to check: $g r^k g^{-1} = r^j \ \forall g \in D_n$ $\quad r r^k r^{-1} = r^k \in R$

$s r^k s^{-1} = s r^k s = \underbrace{(srs)(srs)(srs) \dots (srs)}_{k} = \underbrace{r^{-1} r^{-1} \dots r^{-1}}_{k} = r^{-k} \in R$

$srs = r^{-1}$

Cosets in D_n with respect to R:

$1R = \{1, r, r^2 \dots r^{n-1}\} = r^2 R = \{r^2, r^3, \dots r^{n-1}, 1, r\}$

$sR = \{s, sr, sr^2 \dots sr^{n-1}\}$ $\quad D_n = (1R) \cup (sR)$ disjoint union

2. Let $K = \langle s \rangle = \{1, s\} \subset D_n$. Then K is not normal in D_n:

$s s s^{-1} = s$; $\quad r s r^{-1} = s r^{-1} r^{-1} = s r^{-2} \notin K$

$srs = r^{-1} \Rightarrow rs = sr^{-1}$

Poll: normal subgroups in D_n

Consider the following subgroups in dihedral groups:

(1). $\{1, r^3, r^6\} \subset D_9$ ✓ $\longrightarrow sr^3s = r^{-3} = r^6 \in$ subgp $\Rightarrow$ normal

(2). $\{1, sr\} \subset D_6$ ✗ $\longrightarrow ssrs = rs \notin$ subgp $\Rightarrow$ not normal

(3). $\{1, sr^5\} \subset D_6$ ✗ $\longrightarrow ssr^5s = sr^{-5} \notin$ subgp $\Rightarrow$ not normal

(4). $\{1, r^2, r^4, r^6\} \subset D_8$ ✓ $\longrightarrow sr^{2k}s = r^{-2k} \in$ subgp $\Rightarrow$ normal

(5). $\{1, sr^4\} \subset D_8$. ✗ $\longrightarrow ssr^4s = sr^{-4} = sr^4 \in$ subgp

but $rsr^4r^{-1} = rsr^3 = sr^{-1}r^3 = sr^2 \notin$ subgp

Poll: The following subgroups in the list are normal:

A: Only (1).

B: Only (2), (3) and (5).

C: Only (5).

D: Only (1) and (4).

E: Only (1), (4) and (5).

Quotient groups: group of cosets with respect to a normal subgroup

Proposition

If $H \trianglelefteq G$ is a normal subgroup, then the set of left H-cosets in G naturally forms a group. Namely, define $(xH) \cdot (yH) = (xyH)$, then $(1H)$ is the neutral element and $(xH)^{-1} = (x^{-1}H)$. The group law on the set of left H-cosets G/H is well defined and gives rise to a group structure on G/H.

Need to check: the group law does not depend on the choice of representatives of cosets.

Suppose $x' \in xH$, $y' \in yH$. Need to show: $x'y' \in xyH$

$x' = xh_1$, $y' = yh_2$ $\Rightarrow$ $x'y' = xh_1yh_2 = x\overbrace{y\,y^{-1}}^{1}h_1y\,h_2 = xyh_3h_2 \in xyH$.

$h_1, h_2 \in H$

$y^{-1}h_1y = h_3 \in H$ because H is normal.

$\Rightarrow$ indeed $x'y' \in xyH \Rightarrow$ the group law is well defined.

$\blacksquare$

Example: Cosets of $R = \{1, r, \dots r^{n-1}\}$ in D_n.

$1R = \{1, r, \dots r^{n-1}\}$
$sR = \{s, sr, \dots sr^{n-1}\}$
They form a group, called the quotient group D_n/R with elements the left R-cosets and the group law defined by the proposition above.

Neutral element: coset of 1.

$(1R)(sR) = (sR)$
$(sR)(1R) = (sR)$
$(sR)(sR) = (1R)$
$(1R)(1R) = (1R)$

You can check it taking different representatives of the cosets:

Ex: $g_1 \in sR \quad g_2 = 1R \Rightarrow$

$\underbrace{sr^i}_{g_1} \cdot \underbrace{r^j}_{g_2} = sr^{i+j} \in sR \Rightarrow (sR)(1R) = (sR)$

$g_2 g_1 = r^j s r^i = s\underbrace{(s r^j s)}_{r^{-j}} r^i = s r^{-j} r^i = s r^{i-j} \in sR \Rightarrow (1R)(sR) = (sR).$

Obtain a group $D_n/R \simeq C_2 = \langle t \mid t^2 = 1 \rangle = \{1, t\}. \approx \{(1R), (sR)\}$

Summary of elements of group theory

1. A subgroup $H \trianglelefteq G$ is normal if $ghg^{-1} \in H$ for any $g \in G$, $h \in H$.
2. A quotient group G/H is a group of left cosets with respect to a normal subgroup $H \trianglelefteq G$. Multiplication: $(xH)(yH) = (xyH)$.
   $|G| = |G/H| \cdot |H| = [G : H] \cdot |H|$ by Lagrange's theorem.
3. If $\phi : G_1 \to G_2$ is a group homomorphism, then $\ker\phi \trianglelefteq G_1$ is normal in G_1.
4. Any subgroup $H \subset G$ is normal in an abelian group G.
5. $D_n = \langle s, r \mid s^2 = 1, r^n = 1, srs = r^{-1} \rangle$, $n \geq 3$ is an example of a non-abelian group.
   Then $R = \langle r \mid r^n = 1 \rangle \trianglelefteq D_n$ and $D_n/R \simeq C_2$ cyclic group of 2 elements.
   $|D_n| = [D_n : R] \cdot |R| = 2 \cdot n = 2n$.