Groups

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ $\qquad$ $\mathbb{Q}^+ = \{ q \in \mathbb{Q} \mid q > 0 \}$

$(\mathbb{Z}, +)$ $\qquad$ $(\mathbb{Q}^+, \cdot)$

$(a+b)+c = a+(b+c)$ associativity $\qquad$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$x + 0 = 0 + x = x$ $\quad \exists$ identity element $\quad$ $1 \cdot q = q \cdot 1 = q$

$a + (-a) = 0$ $\quad \exists$ inverses $\quad$ $q \cdot \frac{1}{q} = 1$

Def: $(M, \odot)$ $\to$ M is a set, $\to$ $\odot : M \times M \to M$ is a group if $(M, \odot)$ satisfies the following 3 properties:

(ASOC): $\forall x, y, z \in M \quad (x \odot y) \odot z = x \odot (y \odot z)$

(ID) $\quad \exists e \in M . \forall x \in M \quad e \odot x = x \odot e = x$
$\quad$ ↳ identity / neutral element

(INV) $\quad \forall x \in M . \exists y \in M . \quad x \odot y = y \odot x = e$
$\quad$ ↳ "inverse of x" $\quad$ ↳ id

Examples of groups $\to$ (COM) $\forall a, b \in M \quad a \odot b = b \odot a$
↳ commutative → Abelian

$\boxed{(\mathbb{Z}, +), \quad (\mathbb{Q}^+, \cdot), \quad (\mathbb{Q} \setminus \{0\}, \cdot)}$ $\qquad$ $\cancel{(\mathbb{Q}, \cdot)}$

$\to$ (= nonzero determinant)

- $GL(n)$ ... set of all $n \times n$ invertible matrices

$(GL(n), \cdot)$ is a group $\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$

↳ matrix mult $\qquad$ $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \\ & \end{pmatrix}$

"general linear group"

ex... (cont')

X ... set

$\Pi(X)$ ... all permutations of X

$(\Pi(X), \circ)$

↳ function composition

id_X: $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 3$

$f(g \circ h(x))$ $\quad (f \circ g)(h(x))$

not commutative

Groups in cryptography

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

$(\mathbb{Z}_n, +)$

↳ addition modulo n

$\{x \in \{0,\dots,n-1\} \mid \gcd(x,n)=1\} = \mathbb{Z}_n^\times$

$(\mathbb{Z}_n^\times, \cdot)$

↳ multiplication modulo n

$0 < k < n$

$(n-k)+k = n \pmod n$
$= 0$

$\mathbb{Z}_4^\times = \{\cancel{0}, 1, \cancel{2}, 3\}$ $\quad 3\cdot 3 = 9 \equiv 1 \pmod 4$

inverse of $2 \pmod 4$?

$2\cdot 0 = 0 \pmod 4$
$2\cdot 1 = 2 \pmod 4$
$2\cdot 2 = 4 = 0 \pmod 4$
$2\cdot 3 = 6 = 2 \pmod 4$

Elliptic curve groups.

$(M, \odot)$

$\boxed{G = (M,\cdot) \quad x \in G \;\dots\; G = (M,\cdot),\ x \in M}$

Additive notation $G=(M,+)$		Multiplicative notation $G=(M,\cdot)$
$+$	group op symbol	$\cdot$
0	identity elem. notation	1
$-x$	symbol for inversion $x \in M$	x^{-1}
$n\cdot x = \underbrace{x+x+x \dots +x}_{n\text{-times}}$	n-fold application of group op on $x \in M$: $\underbrace{x \odot x \odot x \dots \odot x}_{n\text{-times}}$	$x^n = \underbrace{x\cdot x \cdots x}_{n\text{-times}}$

$\underbrace{(x^2)^3}_{(x\cdot x)\cdot(x\cdot x)\cdot(x\cdot x)} = x^6$

Reasoning abt groups

Eg.: In every group G there is a unique identity element.

Proof: Assume there are 2 identity elem's $x, y \in G$.

$$\forall a \in G: \boxed{x \cdot a = a \cdot x = a} \leftarrow \text{put } a = y$$

$$y \cdot a = a \cdot y = a \leftarrow \text{put } a = x$$

$$x = x \cdot y = y$$

Practice group notation

Let $x \in G$, let $m, n \in \mathbb{N}$. $\underbrace{(x^m)^n}_{}$ $= x^{m \cdot n}$

$\overbrace{x \cdots x}^{m\text{-times}}$

$$\underbrace{(x^m) \cdots (x^m)}_{n\text{-times}}$$

$$\underbrace{x \cdot \ldots \cdot x}_{(m \cdot n)\text{-times}}$$

$x \in G$, $m, n \in \mathbb{N}$. $\underline{x^m} \cdot \underline{x^n} = x^{m+n}$

$$e = \cancel{x^{-1}} \cdots \cancel{x^{-1}} \cdot \cancel{x^{-1} \cdot x} \cdot \cancel{x} \cdots \cancel{x}$$

Let $x \in G$, let $y = x^n$ for some $n \in \mathbb{N}$.

Suppose we know x^{-1}.

How can we compute y^{-1}?

$$(x^{-1})^n \cdot y = (x^{-1})^n \cdot x^n$$

$$y^{-1} = (x^n)^{-1}$$

$$= \underline{(x^{-1})^n} = y^{-1}$$

x^{-n}

Let $x, y \in G$. Let $k \in \mathbb{N}$. → not for general groups

$$(x \cdot y)^k \neq x^k \cdot y^k$$ → only in Abelian groups

$$\underbrace{(x \cdot y) \cdot x \cdot y \cdot \ldots \cdot x \cdot y}_{k \text{ times}}$$

Finite Abelian groups.

Note: $(\mathbb{Z}_n^{\times}, \cdot)$ and EC groups are finite Abelian groups.

Definition: Let G be a finite ~~Abelian~~ group.
The order of G is the number of elem's of G, i.e. $|G|$.

Ex: $(\mathbb{Z}_{13}^{\times}, \cdot)$ has order 12.

$$(\mathbb{Z}_{15}^{\times}, \cdot) = \{1, 2, 4, 7, 8, 11, 13, 14\} \text{ order } 8$$

Lemma: Let G be a finite group. Then for every $x \in G$ there exists a positive $n \in \mathbb{N}^+$ such that $x^n = 1$.
Moreover, n can be chosen to be at most $|G|$.

Proof: Consider sequence $\underbrace{x, x^2, x^3, \ldots, x^{|G|}, x^{|G|+1}}_{|G|+1}$

only $|G|$ elem's available

$$\Rightarrow \exists\, i < j \quad x^i = x^j \,/\, \cdot x^{-i} \quad 1 \leq i < j \leq |G|+1$$

$$1 = x^{\underbrace{j-i}_{>0}} \} \leq |G|$$

Def: Let G be a finite group and $x \in G$.
The order of x in G, denoted as $\mathrm{ord}(x)$ is the smallest positive $n \in \mathbb{N}$ s.t. $x^n = 1$.

$$\boxed{x^{\mathrm{ord}(x)} = 1.}$$

$1 \leq \mathrm{ord}(x) \leq |G|$.

Lagrange's theorem: Let G be a finite group and $x \in G$.
Then $\mathrm{ord}(x) \mid |G|$

"divides"

Corollary: $x^{|G|} = 1$.

Proof: $x^{|G|} = x^{\mathrm{ord}(x) \cdot k} = \Big(\underbrace{x^{\mathrm{ord}(x)}}_{1}\Big)^k = 1^k = 1$

$|G| = \mathrm{ord}(x) \cdot k$

Example $(\mathbb{Z}_{13}^{\times}, \cdot)$

$$5^{26} = 5^{2 \cdot 12 + 2} = \underbrace{5^{2 \cdot 12}}_{\underbrace{(5^{12})^2}_{1}} \cdot 5^2 = 5^2$$

Important takeaway: in a finite group

$$\underline{\underline{x^n = x^{(n \bmod |G|)}}}$$

Inverses in $(\mathbb{Z}_n^\times, \cdot)$

Bézout's identity:

$\forall a, b \in \mathbb{Z}$ there exit $x, y \in \mathbb{Z}$ s.t.

$$a \cdot x + b \cdot y = \gcd(a, b)$$

and moreover, x, y can be computed by Extended Euclidian algorithm.

How to compute a^{-1} for $a \in \mathbb{Z}_n^\times$

We know: $\gcd(n, a) = 1$

Bézout $\Rightarrow \exists x, y$ s.t. $a \cdot x + \cancel{n \cdot y} = 1 \pmod n$

$$a \cdot \underset{\substack{\parallel \\ a^{-1} \pmod n}}{x} = 1 \pmod n$$