Sept24

Wednesday, September 23, 2020 8:42 AM

Groups

Def A Group is a set G with a rule $*$ for combining elts, $a,b \in G$, $a*b \in G$, satisfying

1) There exist $e \in G$ s.t. $e*a = a = a*e$
2) Any $a \in G$, there is a (unique) inverse a^{-1} s.t. $a*a^{-1} = e = a^{-1}*a$
3) $a*(b*c) = (a*b)*c$.

If also
4) $a*b = b*a$
then G is commutative

Examples

1) $\mathbb{F}_p^*$ $\quad e = 1 \quad * = \times$
2) $\mathbb{Z}/n\mathbb{Z}$ $\quad e = 0 \quad * = +$
3) $G_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R},\ ad - bc \neq 0 \right\}$
$G_1 \subseteq M_2(\mathbb{R})$
$*$ = matrix multiplication.
$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
check $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ✓
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
check $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
check
$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ $\neq$
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$
4) $GL_n(\mathbb{R}) = \{ n \times n \text{ matrices w/ nonzero det} \}$
5) $GL_n(\mathbb{F}_p)$
$\hookrightarrow GL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{F}_p,\ ad - bc \neq 0 \right\}$
Check This is a group
$|GL_2(\mathbb{F}_p)| \leq p^4$

If G a group, $a \in G$, $n > 0$

define $a^n = \underbrace{a*a*a*\cdots*a}_{n\text{-times}}$

$a^0 = 1$

$a^{-n} = (a^{-1})^n$

Def The Discrete Log Problem for G is given $g \in G$, $h \in G$. Find x s.t. $g^x = h$.

Warning In $\mathbb{F}_p^*$ $g^n = g^n$
But in $\mathbb{Z}/N\mathbb{Z}$ ← Additive group
"$g^n = g+g+\cdots+g = n \cdot g$"
(n-times)

Def G a group. $g \in G$.
The order of g is
$|g| = \min\{d > 0 \mid g^d = e\}$
or ∞ if $g^d \neq e$ all $d > 0$

Example
$G = \mathbb{Z}$, $g = 1$. $|g| = \infty$
b/c $1+1+1+1+\cdots \neq 0$

* Any $g \in \mathbb{F}_p^*$. $\begin{cases} 1)\ |g| < \infty & (FLT \Rightarrow g^{p-1} = 1) \\ 2)\ |g| \mid p-1 & \\ 3) \text{If } g^k = 1 \text{ then } |g| \mid k \leftarrow \end{cases}$

Prop (properties of exponentiation)
Let G be a finite group.
$|G| = N$.
$g \in G$.
1) $|g| = d < \infty$
2) If $g^k = e$ then $d \mid k$
3) $g^N = e$ ← Fermat
4) $d \mid N$

$\left.\begin{matrix} g^N = 1 \\ \Rightarrow d \mid N \end{matrix}\right\}$

Pf (1) Need to show a positive power of g is identity.
List $g, g^2, g^3, \cdots$ must repeat
Say $g^i = g^j$ some $j > i$
$g^i * (g^i)^{-1} = (g^i)(g^i)^{-1} = e$
$g^{j-i} = g^{j-i}$

---

(2) $g^k = e$
Long divide $k \div d$
$k = dq + r \quad 0 \leq r < d$
$e = g^k = g^{dq+r} = g^{dq} * g^r = g^r$
But d was min so $r = 0$
so $k = dq$ done.
(3) $g^N = 1$ (G commutative)
$G_1 = \{a_1, a_2, \cdots, a_N\}$
$g*G_1 = \{g*a_1, g*a_2, \cdots, g*a_N\}$
If all elts of $g*G_1$ are different → $G_1 = g*G_1$
$g*a_i = g*a_j$
$g^{-1}*g*a_i = g^{-1}*g*a_j$
$e*a_i = a_j$
$a_i = a_j \Rightarrow i = j$
$a_1 * a_2 * \cdots * a_N = g*a_1 * g*a_2 * g*\cdots*g*a_N$
$= a_1 * \cdots * a_N * g^N$
$e = e * g^N = g^N$.
(4) immediate from 2 & 3

Time Complexity

Example Solving DLP $g \in \mathbb{F}_p^*$

Goal: Solve $g^x \equiv h \bmod p$

① $g, g^2, g^3, \cdots g^x$ Done takes $\approx p$ steps multiplications
$\uparrow_h$
If $p \approx 2^{80}$ too long.

② Choose random x.
Compute g^x ← $\sim \log p$
Check if its h.
$\left.\begin{matrix} \\ \\ \end{matrix}\right\} \approx p$ times
$\sim p \cdot \log p$ "steps"
task 2 $\log p$ step?

"a small multiple of $p \cdot \log p$ steps ..."

③ $g, g^2, g^4, g^8, \cdots$
Took $\approx 2^{80}$ multiplications
But Multiply 2 #s k bits long takes $\approx k^2$ steps. ← additions
This took $(\sim) k^2 \cdot 2^k$ steps & in terms of $k = \#$ bits
$(\log_2(p))^2 \cdot p$ ← in terms of p

Order notation

For $k >> 0$
2^k, $5 \cdot 2^k$, $11 \cdot 2^k$ similar.
$\uparrow$ 1000 yrs, $\uparrow$ 5000 yrs

Def f, g functions of a positive variable x, with values in $\mathbb{R}_{\geq 0}$
Then f is big O of g
$f(x) = O(g(x))$
if there is constants C & $N > 0$
s.t. for all $x > N$
$f(x) \leq C g(x)$

Rmk f is a bounded function.
$\Rightarrow f = O(1)$

Pf $C = \max f(x) \Rightarrow f(x) \leq C$

Prop
Suppose $\lim_{x\to\infty} \frac{f(x)}{g(x)} < \infty$
Then $f(x) = O(g(x))$
Pf $L = \lim_{x\to\infty} \frac{f(x)}{g(x)}$. So any $\varepsilon > 0$
$\exists$ some N_ε s.t. all $x > N$
$\left| \frac{f(x)}{g(x)} - L \right| < \varepsilon = 1$
$\frac{f(x)}{g(x)} - L < 1$
$f(x) < g(x)[L+1]$
C.

Remark Big O notation is an upper bound.
$2 = O(5000^k)$

Def If $f = O(g)$ & $g = O(f)$
then $f = \Theta(g)$. big theta

Prop If $0 < \lim_{x\to\infty} \frac{f(x)}{g(x)} < \infty$
Then $f(x) = \Theta(g(x))$
Pf HW

Examples
$2x^3 - 3x^2 + 7 = \Theta(x^3)$
$\lim_{n\to\infty} \frac{2x^3 - 3x^2 + 7}{x^3} \overset{LH}{=} \frac{12}{6} = 2 < \infty$
② $k^{300} = O(2^k)$
$\lim_{n\to\infty} \frac{k^{300}}{2^k} = \lim \frac{300!}{C \cdot 2^k} = 0$
③ $(x+2)\cos(x^2) = O(x)$
$\because x+2 \leq 2x = O(x)$
But $\lim_{x\to\infty} \frac{(x+2)\cos x^2}{x}$ DNE

Trying to solve some mathematical problem with computation.

	Integer Factorization	DLP
Input	N	$g \in \mathbb{F}_p^*$, h
Output	prime factors	$\log_g x$

Typically
Know time (& space) complexity of algorithm in terms of # bits of input.
↳ "storage size of input"
$N \sim 2^{20}$ vs $N \sim 2 \cdot 2^{20}$
$N \sim 2^{40}$ "twice as big"
Usually $N \sim 2^k \leftrightarrow k = \log_2 N$
Complexity $O(f(x))$ ← "bit complexity"
Sometimes $O(F(N))$ ← "Absolute complexity"

Def Suppose $\exists$ $A > 0$ s.t.
Input $O(k)$ k bits
Alg takes $O(k^A)$ steps.
Then polynomial time solution
$A = 1$ Linear Time
$A = 2$ Quadratic Time.

If $\exists$ $c > 0$ s.t.
If input $O(k)$ bits
alg takes $O(e^{ck})$ steps
Then Exponential Time.

Example Quadratic vs Exponential

k	N	$O(k^2)$	$O(2^k)$
1	2	.0001	.0001
2	2^2	.0004	.0004
5	2^5	.0025	.0032
10	2^{10}	.01	.1024
20	2^{20}	.04	104.8576
50	2^{50}	.25	1.1×10^{13}
100	2^{100}	1	1.2×10^{28}

Moral
Polynomial = fast or easy
Exponential = slow or hard.

Def An alg is subexponential if for all $\varepsilon > 0$ it runs in $O(e^{\varepsilon k})$

Example
$G_1 = \mathbb{F}_p^*$ Solve $g^x = h$
$2^k \leq p \leq 2^{k+1}$
$\Rightarrow$ Problem takes $g, h, p \cong 2^{k+1}$
takes $< 3 \cdot 2^{k+1}$
$= 3 \cdot 2 \cdot 2^k$
$= 6 \cdot 2^k = O(2^k)$ absolute
or $O(k)$ bits.

Solve it
Guess & check takes
$< p$ steps $= O(p)$ absolutely
$= O(2^k)$ bits
exponential
Notice. Each mult of 2 k bit #s takes k^2 steps
Solution $O(k^2 \cdot 2^k) = O(3^k)$
↑ Check
exponential