Groups
An introduction to algebra

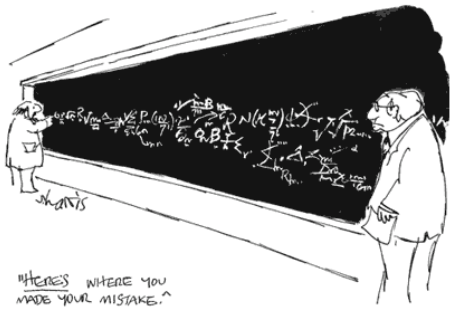
Foundations of Cryptography
Computer Science Department
Wellesley College

Fall 2016

Table of contents

Group theory

- Group theory is certainly one of the most beautiful branches of mathematics.
- Groups play a crucial role in the construction of hard problems*.
- It all starts with a *binary function* which takes as input two elements $a, b \in \mathbb{G}$ and returns a third element, denoted using infix notation, $a \circ b \in \mathbb{G}$.



*Remember, we want these to serve as candidates for one-way functions.

Formally,

Definition 8.9. A *group* is a set $\mathbb{G}$ along with a binary operation $\circ$ for which the following conditions hold:

- *(Closure)* For all $g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
- *(Existence of an Identity)* There exists an *identity* $e \in \mathbb{G}$ such that for all $g \in \mathbb{G}$, $e \circ g = g = g \circ e$.
- *(Existence of an Inverses)* For all $g \in \mathbb{G}$, there exists an element $h \in \mathbb{G}$ such that $g \circ h = e = h \circ g$. Such and H is called an *inverse* of g.
- *(Associativity)* For all $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

When $\mathbb{G}$ has a finite number of elements, we say $\mathbb{G}$ is a *finite group* and let $|\mathbb{G}|$ denote the *order* of the group.
A group $\mathbb{G}$ with operation $\circ$ is *abelian* if the following holds:

- *(Commutativity)* For all $g, h \in \mathbb{G}$, $g \circ h = h \circ g$.

Subgroups

Definition. If $\mathbb{G}$ is a group, a set $\mathbb{H} \subseteq \mathbb{G}$ is a *subgroup* of $\mathbb{G}$ if $\mathbb{H}$ itself forms a group under the same operation associated with $\mathbb{G}$.

Remark. Every group $\mathbb{G}$ has the trivial subgroups $\mathbb{G}$ and $\{e\}$. We call $\mathbb{H}$ a *strict* subgroup of $\mathbb{G}$ if $\mathbb{H} \neq \mathbb{G}$

Remark. We will often use either *additive* $(+)$ notation or *multiplicative* $(\cdot)$ notation for the group operation $\circ$. Don't confuse these with integer addition and multiplication.

Old friends

- $\mathbb{Z}$ is an abelian group under addition and is a subgroup of the following. $\mathbb{Z}$ is not a group under multiplication. Why?
- $\mathbb{R}$ is an abelian group under addition. What about multiplication?
- For $N \geq 2$ the set $\{0, \ldots, N-1\}$ with respect to addition modulo N (i.e., $a + b \stackrel{\text{def}}{=} [a + b \mod N]$) is an abelian group of order N*. We denote this group by $\mathbb{Z}_N$.

*How would we check this?

Cancelation law holds for groups

Lemma 8.13. Let $\mathbb{G}$ be a group and $a, b, c \in \mathbb{G}$. If $ac = bc$, then $a = b$, In particular, if $ac = c$, then a is the identity in $\mathbb{G}$.

Proof.

Group exponentiaion

Definition. It is useful to describe the group operation applied m times to a fixed element.

When using additive notation, we write

$$mg = m \cdot g \stackrel{\text{def}}{=} \underbrace{g + \cdots + g}_{\text{m times}}.$$

When using multiplicative notation, we write

$$g^m \stackrel{\text{def}}{=} \underbrace{g \cdots g}_{\text{m times}}.$$

Remark. The familiar rules of exponentiation hold: $g^m \cdot g^{m'} = g^{m+m'}$; $(g^m)^{m'} = g^{mm'}$; and $g^1 = g$.

Working "modulo the group order in the exponent"

Theorem 8.14. Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$, the order of the group. Then for any element $g \in \mathbb{G}, g^m = 1$.

Proof. We prove the theorem when $\mathbb{G}$ is abelian (though it holds for any finite group). Fix arbitrary $g \in \mathbb{G}$, and let $g_1, \ldots, g_m$ be the elements of $g \in \mathbb{G}$. We show on the board that

$$g_1 \cdot g_2 \cdots g_m = (gg_1) \cdot (gg_2) \cdots (gg_m) = g^m \cdots (g_1 \cdot g_2 \cdots g_m).$$

and conclude (using Lemma 8.13) that $g^m = 1$. □

Corollary 8.15. Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$. Then for any $g \in \mathbb{G}$ and any integer i, we have $g^i = g^{[i \mod m]}$.

One more corollary needed for cryptographic application

Corollary 8.17. Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}| > 1$, Let $e > 0$ be an integer, and define the function $f_e : \mathbb{G} \to \mathbb{G}$ by $f_e(g) = g^e$. If $\gcd(e, m) = 1$, then f_e is a permutation. Moreover, if $d = [e^{-1} \mod m]$ then f_d is the inverse of f_e.

*Proof.**

*Board again?

I've got another riddle for you

- The set $\mathbb{Z}_N = \{0, \ldots, N-1\}$ is a group under addition modulo N.
- Is it a group about under multiplication modulo N as well?
- Well no, since 0 has no inverse. But what if you throw 0 out?

The Group $\mathbb{Z}_N^*$

Proposition 8.7. Let a, N be integers, with $N > 1$. Then a is invertible modulo N if and only if $\gcd(a, N) = 1$.

Definition. Let $N > 1$. Define the set

$$\mathbb{Z}_N^* \stackrel{\text{def}}{=} \{a \in \{1, \ldots, N-1\} \mid \gcd(a, N) = 1\}.$$

Proposition 8.18. Let $N > 1$. Then $\mathbb{Z}_N^*$ is an abelian group under multiplication modulo N.

*Proof.**

*You guessed it: Board.

The Euler phi function

Definition. Define $\phi(N) \stackrel{\text{def}}{=} |\mathbb{Z}_N^*|$, the order of the group $\mathbb{Z}_N^*$.

Puzzlers. What is the value of $\phi(N)$ when $N = p$ is prime? How about when $N = pq$ is the product of two primes? What does $\mathbb{Z}_{10}^*$ look like?

In general,
Theorem 8.19. Let $N = \prod_i p_i^{e_i}$, where the $\{p_i\}$ are distinct primes and $e_i \geq 1$. Then $\phi(n) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Shades of RSA

Theorem 8.14. Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}|$, the order of the group. Then for any element $g \in \mathbb{G}, g^m = 1$.

Corollary 8.21. Take an arbitrary $N > 1$ and $a \in \mathbb{Z}_N^*$. Then

$$a^{\phi(N)} = 1 \mod N.$$

For the specific case that $N = p$ is prime and $a \in \{1, \ldots, p-1\}$, we have

$$a^{p-1} = 1 \mod p$$

*Proof.**

*This one is easy.

More shades

Corollary 8.17. Let $\mathbb{G}$ be a finite group with $m = |\mathbb{G}| > 1$, Let $e > 0$ be an integer, and define the function $f_e : \mathbb{G} \to \mathbb{G}$ by $f_e(g) = g^e$. If $\gcd(e, m) = 1$, then f_e is a permutation. Moreover, if $d = [e^{-1} \mod m]$ then f_d is the inverse of f_e.

Now we have a corollary to a corollary:

Corollary 8.22. Fix $N > 1$. For integer $e > 0$ define $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ by $f_e(x) = [x^e \mod N]$. If e is relatively prime to $\phi(N)$ then f_e is a permutation. Moreover, if $d = [e^{-1} \mod \phi(N)]$ then f_d is the inverse of f_e.

*Proof.**

*This one is easy too. But not as easy as the last one.