GROUP THEORY

MATH 195

The reference for the material covered here is any abstract algebra book; the text by Fraleigh, *A First Course in Abstract Algebra*, sixth edition, is often used at Berkeley.

Group theory

Definition. A *group* is a set $\mathcal{G}$ together with a map $* : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ such that:

- $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathcal{G}$;
- There exists an $e \in G$ such that for all $a \in \mathcal{G}$, $e * a = a * e = a$;
- For all $a \in \mathcal{G}$, there exists an $a' \in \mathcal{G}$ such that $a * a' = a' * a = e$.

If you have never seen groups before and want some practice (or examples), check out SS1.1–1.3 in Fraleigh.

Given an element $b * a$, we can recover b by multiplying by a':

$$(b * a) * a' = b * (a * a') = b * e = b.$$

Notice how this looks like "decryption".

Many of our groups (but not all) will be *abelian*: $a * b = b * a$.

Example. The group of permutations on the (finite) set S, which we called $\mathcal{G} = \operatorname{Sym} S$, has $* = \circ$ (the group law is composition), $e = \mathrm{id}_S$, and $f' = f^{-1}$. This group is nonabelian if S has more than 2 elements. (See §2.1 in Fraleigh.)

Here is notation which is often used for groups:

"Additive" group (usually abelian)	"Multiplicative" group
$* = +$	$* = \circ, \times, \ , \cdot$
$a' = -a$	$a' = a^{-1}$
$e = 0$	$e = 1, \mathrm{id}$
multiple	power
$n \cdot a = na$	a^n
$0a = 0$	$a^0 = 1$
$(-n)a = n(-a)$	$a^{-n} = (a^{-1})^n$
$(m+n)a = ma + na$	$a^{m+n} = a^m a^n$

The Group $(\mathbb{Z}/n\mathbb{Z})^*$

Notice that the set $\mathbb{Z}/26\mathbb{Z} = \{0, 1, 2, \dots, 25\}$ with the addition law (taking the remainder modulo 26) is a group. However, using the multiplication law, it is *not* a group. Although it satisfies the associativity law and has an identity element 1, not every element has an inverse: for example 0 has no inverse. In fact, any element which is not relatively prime to 26—e.g. 12, since if $12a' = 1$ in $\mathbb{Z}/26\mathbb{Z}$,

---

This is some of the material covered January 29, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

then $12a' = 1 + 26n$ for some $n \in \mathbb{Z}$, which is impossible as the left-hand side is even whereas the right hand side is odd.

The set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ is never a group unless $n = 1$, in which the group is just $\{0\}$. The set

$$\mathbb{Z}/n\mathbb{Z} \setminus \{0\} = \{1, 2, \ldots, n-1\}$$

is a group when n is prime and not otherwise: it fails even to be closed—for example, $2 \cdot 13 \equiv 0 \pmod{26}$ is no longer in the group. In general, however, we may take the set of units

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\},$$

and this is a group under multiplication. (For this, see §5.3, especially Theorem 5.3.6 in Fraleigh. It is also covered in SS7.1–7.3 of our text, Stallings.)

Example. Since $26 = 2 \cdot 13$,

$$(\mathbb{Z}/26\mathbb{Z})^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\},$$

a group with 12 elements. We have $7 \cdot 11 \equiv 25 \equiv -1 \pmod{26}$, and therefore $7^{-1} \equiv -11 \equiv 15 \pmod{26}$.

In general, the number of elements of this multiplicative group is

$$\#(\mathbb{Z}/n\mathbb{Z})^* = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Note that this agrees with the above enumeration, since $26(1/2)(12/13) = 12$.