Algebra

The definition of a group

Def. A *group* is a set G closed under a binary operation $\odot$ such that

- *Associative Law:*
  $\forall x, y, z \in G,\ x \odot (y \odot z) = (x \odot y) \odot z.$
- *Identity:* $\exists e \in G$, the *identity*:
  $\forall x \in G,\ e \odot x = x \odot e = x.$
- *Inverse:*
  $\forall x \in G,\ \exists y \in G$ s.t. $x \odot y = y \odot x = e.$
  $y = x^{-1}$ is the *inverse* of x.

Examples: The integers $\mathbb{Z}$, the reals $\mathbb{R}$, and the rationals $\mathbb{Q}$ are groups under addition.

Example: $\mathbb{R} - \{0\}$ under multiplication.

Def. For finite groups, the number of elements in a group G, written $|G|$, is the *order* of the group.

Example: $\mathbb{Z}_n$, the integers modulo n, under addition. The order of $\mathbb{Z}_n$ is n.

Example: $\mathbb{Z}_n^*$, the positive integers less than n which are relatively prime to n, under multiplication. The order of $\mathbb{Z}_n^*$ is $\phi(n)$, where ϕ is the Euler ϕ-function.

The above examples are all *abelian groups* — the operation is commutative: $x \odot y = y \odot x$ for all x, y in the group.
Not all groups are abelian.

Example: S_n, the symmetric group on n letters, is the set of permutations of the set $\{1, 2, ..., n\}$.
S_n is not an abelian group.

Any permutation can be written as a product of cycles.

A *transposition* is a cycle of length 2, (ij). A permutation is *even* iff it can be expressed as a product of an even number of transpositions.

The *symmetric group* of a set X is Sym(X).

Subgroups

Def. Let G be a group, and $H \subseteq G$.
H is a $subgroup$ of G if H itself is a group w.r.t. the operation in G ($H \leq G$). The *order* of a subgroup is its cardinality.

Suppose G is a group and $H \subseteq G$. Then H is a subgroup of G iff the following hold:

- $\forall x, y \in H$, $x \odot y \in H$.
  (H is closed under the group operation.)
- The identity is in H.
- $\forall x \in H$, $x^{-1} \in H$.

Example: Any group is a subgroup of itself.

Example: If e is the identity in G, $\{e\}$ is a subgroup of G.

Example: The even integers are a subgroup of the integers under addition.

Example: $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \right\}$ is a subgroup of S_5.

Example: A_n, the set of all even permutations on n letters, is a subgroup of S_n. It is called the *alternating group* on n letters.

Example: The set $\{0, 5, 10\}$ is a subgroup of $\mathbb{Z}_{15}$ under addition.

Example: The set $\{1, 2, 4\}$ is a subgroup of $\mathbb{Z}_7^*$.

Thm. Suppose S is a nonempty collection of subgroups of a group G. Let $H' = \bigcap_{H \in S} H$. Then H' is a subgroup of G.

Generators

Def. Let H be a subset of a group G, and let S be the collection of all subgroups of G which contain H. Then, $<H>= \bigcap_{G' \in S} G'$ is the *subgroup generated by* H.

$H \subseteq G$.
$<H>= \{h_1 \odot h_2 \odot ... \odot h_n \mid h_i \text{ or } h_i^{-1} \in H \quad \forall i\}$.

Def. A group or subgroup is said to be *cyclic* if it is generated by a single element.
Such an element is a *generator* or
primitive element.

Def. The *order* of an element of a group G is the order of the subgroup that element generates.

Thm. Suppose G is a group with identity e, and $g \in G$ has finite order m. Then m is the least positive integer such that $g^m = e$.

Example: The set $\{2\}$ generates the subgroup $\{1, 2, 4\}$ of $\mathbb{Z}_7^*$.
Thus, it is a cyclic subgroup.
The order of the element 2 is 3.
The set $\{3\}$ generates all of $\mathbb{Z}_7^*$,
so it is a cyclic group.

Fact. $\mathbb{Z}_p^*$ is cyclic whenever p is prime.

Lagrange's Theorem

Def. Let $H \leq G$, $x \in G$. $Hx = \{h \odot x \mid h \in H\}$ is a *right coset* of H in G.

Lemma Let $H \leq G$. All right cosets of H contain $|H|$ elements.

The relation $R =$
$\{(a, b) \mid a$ and b are in the same right coset of $H\}$
is an equivalence relation.

Lemma Let H be a subgroup of G, $x, y \in G$. Then either $Hx = Hy$ or $Hx \cap Hy = \emptyset$.

These two lemmas tell us that the group G must be a disjoint union of right cosets of any subgroup H, all of which have the same size.

Thm. [Lagrange] If G is a finite group and $H \leq G$, then the order of H divides the order of G.

Corollary Let G be a finite group and $g \in G$. The order of the element g divides the order of the group G.

Corollary Suppose $|G| = n$ and $g \in G$. Then $g^n = e$, where e is the identity in G.
Pf. Let s be the order of the subgroup generated by g. By a previous theorem, $g^s = e$, where e is the identity. By Lagrange's Theorem, s divides n, so there is an integer c such that $n = sc$. Note that $g^n = g^{sc} = (g^s)^c = e^c = e$, so the corollary follows. □

Thm. [Fermat's Little Theorem] If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Using this same group theory, we can show that encryption with RSA, followed by decryption with RSA yields the original message, if the message is less than n and relatively prime to n.

$n = pq$ where p and q are large primes.
$|\mathbb{Z}_n^*| = \phi(n) = (p-1)(q-1)$.
If the message M is less than n and relatively prime to n, $M \in \mathbb{Z}_n^*$.
$ed \equiv 1 \pmod{(p-1)(q-1)}$,
so $\exists k \in \mathbb{Z}$ s.t. $ed = 1 + k(p-1)(q-1)$.

If $C \equiv M^e \pmod{n}$, then $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot M^{k(p-1)(q-1)} \equiv M \cdot (M^{\phi(n)})^k \equiv M \cdot 1^k \equiv M \pmod{n}$.

Rings and fields

Def. A *ring* is a set R closed under two binary operations $+$ and $\bullet$ s.t.

- R1. R is an abelian group with respect to the operation $+$.
- R2. The operation $\bullet$ is associative.
- R3. [Distributive Laws] $\forall x, y, z \in R$, the following hold:

$$\begin{aligned} x \bullet (y + z) &= x \bullet y + x \bullet z \\ (y + z) \bullet x &= y \bullet x + z \bullet x \end{aligned}$$

The first operation $+$ is called addition and the second operation $\bullet$ is called multiplication.

Example: $\{0\}$ is the *trivial ring*.
$0 + 0 = 0$ and $0 \bullet 0 = 0$.
A *nontrivial ring* is a ring with more than one element.

The identity element with respect to addition is called *zero*, and all other elements are called *nonzero elements*.

If the ring R has an identity element i with respect to multiplication, then for all $x \in G$, $i \bullet x = x \bullet i = x$, and R is said to be a *ring with identity*. This identity is denoted by 1.

The ring R is *commutative* if for all $x, y \in R$, $x \bullet y = y \bullet x$.

Examples: $\mathbb{Z}$ and $\mathbb{R}$ are both commutative rings with identity.

Def. A *field* is a nontrivial commutative ring with identity in which every nonzero element has a multiplicative inverse.

Examples: $\mathbb{R}$ is a field and $\mathbb{Q}$ is a field, but $\mathbb{Z}$ is not.

Example: $\mathbb{Z}_n$ is a field when n is prime. It is a ring when n is composite, but not a field.