Abstract Algebra

Most of the number theory we have done so far can be viewed as special cases of very general phenomena.

Either the ocean of specific examples may obscure the underlying abstraction, *or* all these examples may forcefully suggest looking for that underlying unification.

Understanding the abstractions is not strictly necessary for understanding the applications to cryptology.

... but without understanding the unifying abstractions one is stuck with a long list of similar but different examples to remember.

Abstract algebra is relatively modern, only developing since about 1840, and recognized as a coherent subject roughly 1920. Modern times by mathematical standards.

Groups

A **group** is a set G with a single **binary operation** (two inputs from G, output an element of G) for the moment denoted $*$, and an **identity element** e, satisfying properties

• Property of the identity: $e * g = g * e = g$ for all $g \in G$

• Existence of inverses: For every g in G there is $h \in G$ such that $h * g = g * h = e$. This h is called an **inverse** of g, and is often denoted g^{-1}.

• Associativity: $(g * h) * k = g * (h * k)$ for all $g, h, k \in G$

The notation g^{-1} would be inappropriate except that we can prove (below) that *each group element has exactly one inverse.*

If the operation $g * h$ is *commutative*, that is, if $g * h = h * g$ then the group is **abelian**. In that case, often the operation denoted *addition* and the identity is written as 0 instead of e. If the group operation is written as *addition*, then the inverse is written as

$$\text{inverse of } g = -g$$

Often the operation is written as multiplication

$$g * h = g \cdot h = gh$$

and the identity is written 1. For $0 \leq n \in \mathbf{Z}$

$$g^n = \underbrace{g * \ldots * g}_{n}$$

$$g^{-n} = \underbrace{g^{-1} * \ldots * g^{-1}}_{n}$$

Examples

In the following, it is easy to verify the properties necessary for the things to qualify as *groups*:

$\mathbf{Z}$ with usual addition $+$. Identity is 0 and inverse of x is $-x$. Abelian.

Even integers $2\mathbf{Z}$ with addition $+$. Identity is 0 and inverse of x is $-x$. Abelian.

Rational numbers $\mathbf{Q}$ with addition. Identity is 0, inverse of x is $-x$. Abelian.

Nonzero rational numbers $\mathbf{Q}^\times$ with multiplication. Identity is 1, inverse of x is $1/x$. Abelian.

Real numbers $\mathbf{R}$ with addition. Identity is 0, inverse of x is $-x$. Abelian.

Nonzero real numbers $\mathbf{R}^\times$ with multiplication. Identity is 0, inverse of x is $-x$. Abelian.

Additive group of Z mod m: $\mathbf{Z}/m$ with addition-mod-m as operation. Identity is 0-mod-m and the inverse of x-mod-m is $(-x)$-mod-m. Abelian.

Example: With addition,

$$\mathbf{Z}/5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Example: With addition,

$$\mathbf{Z}/6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

Multiplicative group $\mathbf{Z}/m^\times$ of Z mod m: Integers mod m *relatively prime to* m, with multiplication-mod-m as operation. Identity is 1-mod-m. Abelian.

Example: With multiplication,

$$\mathbf{Z}/5^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Example: With multiplication,

$$\mathbf{Z}/6^\times = \{\bar{1}, \bar{5}\}$$

Vectors in n-space $\mathbf{R}^n$ with vector addition. Identity is 0 vector. Inverses are negatives.

The set $GL(2, \mathbf{R})$ of invertible two-by-two real matrices, with group law matrix multiplication. The identity is the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Existence of inverses is part of the definition. The associativity is not obvious from the definition. This group is not abelian.

Permutations of a set form a group, with operation being *composition* (as functions) of permutations. The do-nothing permutation is the identity. If there are more than two elements, the group of permutations is non-abelian.

Not every binary operation is associative.

Subtraction is not generally associative, in the ordinary integers. For example

$$(5 - 2) - 1 = 3 - 1 = 2$$

but

$$5 - (2 - 1) = 5 - 1 = 4$$

Division is not generally associative, in the rational numbers. For example

$$(2 \div 2) \div 2 = 1 \div 2 = 1/2$$

while

$$2 \div (2 \div 2) = 2 \div 1 = 2$$

Proving some obvious things

Some assertions about groups may seem silly, but it is worth thinking about their proofs, because of the **universality** in which we are asserting them.

That is, things which may be mildly silly to bother with in simple computational examples are more worthwhile to consider if we can establish decisive facts once and for all.

Proposition: There is exactly one element of a group G having the property of the identity.

Proof: Suppose that $e * g = g$ for all $g \in G$, and $g * e' = g$ for all $g \in G$. Then

$$\begin{aligned} e &= e * e' \text{ (by property of } e') \\ &= e' \text{ (by property of } e) \end{aligned}$$

Thus $e = e'$. ///

Proposition: An element g in a group G has exactly one inverse.

Proof: Let $h * g = e$, $g * k = e$. Then

$$h = h * e \text{ (property of } e\text{)}$$

$$\begin{aligned} &= h * (g * k) \text{ (property of } k\text{)} \\ &= (h * g) * k \text{ (associativity)} \\ &= e * k \text{ (property of } h\text{)} \\ &= k \text{ (property of } e\text{)} \end{aligned}$$

So $h = k$. ///

The point of this and the previous proposition is that we do not have to add a further axiom to be sure that there's only one identity or only one inverse. These properties *always* follow.

A subset H of a group G is a **subgroup** if
• H contains the identity e
• H is **closed under inverses**, meaning that if $h \in H$ then $h^{-1} \in H$
• H is **closed under multiplication**, meaning that if $g, h \in H$ then $g * h \in G$

Example: The set $\{e\}$ is a subgroup of any group G.

Example: The even integers $2\mathbf{Z}$ form a subgroup of the group $\mathbf{Z}$ of integers with addition.

Example: The *odd* integers are **not** a subgroup of the group $\mathbf{Z}$ of integers with addition, since 0 is not among them. Also, they are not closed under addition.

Example: The nonzero integers are not a subgroup of the group of nonzero rationals $\mathbf{Q}^\times$ with multiplication, since most inverses are not in that set. For example, $3^{-1} \notin \mathbf{Z}$.

Example: The **cyclic subgroup** $\langle g \rangle$ **generated by** an element g of G consists of e, g, g^{-1}, g^2, g^{-2}, etc. Not all the powers of g need be different.

Example: The set $H = \langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{4}\}$ is a subgroup of $\mathbf{Z}/7^{\times}$. Check by brute force (don't do this!)

• certainly $\bar{1}$ is in H, by definition.

• closure under inverses: $2 \cdot 4 = 8 = 1 \bmod 7$, and $1 \cdot 1 = 1 \bmod 7$, so everything in H has an inverse in H.

• closure under multiplication: multiplying anything by 1 gives the same thing. Multiplying $2 \cdot 2 = 4 \bmod 7$. $2 \cdot 4 = 8 = 1 \bmod 7$. $4 \cdot 4 = 16 = 2 \bmod 7$. Ok!

Example: For an abelian group, if we use additive notation, the **cyclic subgroup** $\langle g \rangle$ **generated by** an element g of G consists of 0, g, $-g$, $2g$, $-2g$, etc. Not all the powers of g need be different.

Proposition: The cyclic subgroup $H = \langle g \rangle$ generated by an element g of a group G really is a subgroup.

Proof: This is a dressed-up version of the so-called *Laws of Exponents*, which should really be called *Properties of Exponents*.

$$\begin{array}{rcccc} 1 & = & g^0 & \in H & \text{(convention)} \\ g^m * g^n & = & g^{m+n} & \in H & \text{(ind'n, cases)} \\ (g^n)^{-1} & = & g^{-n} & \in H & \text{(ind'n)} \end{array}$$

Thus, we have proven: presence of the identity in the subset, closure under multiplication, and closure under inverses, so H is a subgroup. ///

Order

The **order** $|G|$ of a *group* G is its number of elements. The **order** $|g|$ of an *element* $g \in G$ is the smallest positive integer ℓ (if it exists at all!) such that $g^\ell = e$.

Example: In the group $\mathbf{Z}/9$ with addition, by brute force the element $\bar{3}$ has order 3:

$$1 \cdot 3 = 3 \neq 0 \bmod 9$$
$$2 \cdot 3 = 6 \neq 0 \bmod 9$$
$$3 \cdot 3 = 9 = 0 \bmod 9$$

In that same group, the order of $\bar{4}$ is 9:

$$\begin{aligned}
1 \cdot 4 &&&= 4 &&\neq 0 \bmod 9 \\
2 \cdot 4 &&&= 8 &&\neq 0 \bmod 9 \\
3 \cdot 4 &= 12 &&= 3 &&\neq 0 \bmod 9 \\
4 \cdot 4 &= 16 &&= 7 &&\neq 0 \bmod 9 \\
5 \cdot 4 &= 20 &&= 2 &&\neq 0 \bmod 9 \\
6 \cdot 4 &= 24 &&= 6 &&\neq 0 \bmod 9 \\
7 \cdot 4 &= 28 &&= 1 &&\neq 0 \bmod 9 \\
8 \cdot 4 &= 32 &&= 5 &&\neq 0 \bmod 9 \\
9 \cdot 4 &= 36 &&&&= 0 \bmod 9
\end{aligned}$$

Example: We determine the order of $\bar{2}$ in $\mathbf{Z}/11^\times$ by brute force:

$$\begin{array}{lllllll}
2^1 & & & = & 2 & \neq & 1 \bmod 11 \\
2^2 & & & = & 4 & \neq & 1 \bmod 11 \\
2^3 & & & = & 8 & \neq & 1 \bmod 11 \\
2^4 & = & 16 & = & 5 & \neq & 1 \bmod 11 \\
2^5 & = & 32 & = & 10 & \neq & 1 \bmod 11 \\
2^6 & = & 64 & = & 9 & \neq & 1 \bmod 11 \\
2^7 & = & 128 & = & 7 & \neq & 1 \bmod 11 \\
2^8 & = & 256 & = & 3 & \neq & 1 \bmod 11 \\
2^9 & = & 512 & = & 6 & \neq & 1 \bmod 11 \\
2^{10} & = & 1024 & & & = & 1 \bmod 11
\end{array}$$

Thus, the order of $\bar{2}$ in $\mathbf{Z}/11^\times$ is 10. In other words, 2 is a **primitive root** modulo 11.

Unlike additive problems, it does not seem that there is any easy way to anticipate in advance the order of elements of $\mathbf{Z}/m^\times$.

Lagrange's Theorem

This is the first real theorem in group theory, and is ubiquitous in mathematics.

Theorem: Let G be a finite group. The order of a subgroup H of G *divides* the order of G.

Proof: Define the **left coset** gH of H by an element g of G to be

$$gH = \{gh : h \in H\}$$

We will show that the union of all of the cosets of H is all of G, that any two cosets are either disjoint or exactly the same, and that all cosets of H have the same number of elements, the order $|H|$ of H. If we do this, then

$$|G| = (\text{num. distinct cosets } H) \cdot |H|$$

First, certainly

$$g = g \cdot e \in gH$$

Thus, every $g \in G$ is in coset gH.

Second, suppose $xH \cap yH \neq \phi$. Anything in the intersection is expressible two ways

$$xh = yk$$

for some $h, k \in H$. Right multiply by $k^{-1} \in H$ to obtain

$$xhk^{-1} = y$$

Thus, for *any* $\ell \in H$,

$$y\ell = xhk^{-1}\ell$$

so $yH \subset xH$. Symmetrically, $xH \subset yH$, so $xH = yH$. Thus, if two cosets overlap they are equal.

Finally, we claim that all cosets have $|H|$ elements. Indeed, the map $f : H \to gH$ by $f(h) = gh$ is a bijection. Indeed, if $gh_1 = gh_2$, left multiplication by g^{-1} shows that $h_1 = h_2$, so f is an injection. And, given $gh \in gH$, surely $f(h) = gh$, so f is a surjection. So f is a bijection.

In summary: Every element of G lies in *some* coset of H. Distinct cosets are disjoint. Any coset has exactly $|H|$ elements. Thus, we can count (without repetition) elements in G by the cosets in which thy lie

$$|G| = (\text{num. distinct cosets } H) \cdot |H|$$

which is Lagrange's theorem. ///

Abstracting Euler's Theorem

Proposition: The order ℓ of an element g of a group G is equal to the order of the cyclic subgroup $\langle g \rangle$ generated by g. In particular, $e, g, g^2, \ldots, g^{\ell-1}$ is an irredundant list of elements in $\langle g \rangle$. And $g^n = e$ if and only if $\ell | n$.

Proof: Prove the last assertion first. Suppose $g^n = e$. Write $n = q\ell + r$ with $0 \leq r < \ell$. Then

$$e = g^n = g^{q\ell+r} = (g^\ell)^q \cdot g^r = e^q \cdot g^r = g^r$$

Thus, by the minimality of ℓ necessarily $r = 0$. That is, $\ell | n$. And if $\ell | n$ the same argument can be run backward to prove that $g^n = e$.

Next, prove that the elements $e, g, g^2, \ldots, g^{\ell-1}$ are distinct. If $g^i = g^j$ for $i < j$, then $e = g^{j-i}$, and by the first part $\ell | (j-i)$. For $0 \leq i < j \leq \ell - 1$ this cannot happen.

Next, prove that any g^n is equal to some one of the $e, g, g^2, \ldots, g^{\ell-1}$. Again, write $n = q\ell + r$ with $0 \leq r < \ell$. Then, as usual,

$$g^n = g^{q\ell+r} = (g^\ell)^q \cdot g^r = e^q \cdot g^r = g^r$$

This proves that $\langle g \rangle$ consists exactly of $e, g, g^2, \ldots, g^{\ell-1}$.

Finally, in particular, the order of the *subgroup* $\langle g \rangle$ is the number of these elements $e, g, g^2, \ldots, g^{\ell-1}$, which is ℓ, the order of the *element* g. ///

Corollary: *(Euler's Theorem)* Let $\varphi(n)$ be Euler's ϕ-function of n. For b relatively prime to n,

$$b^{\varphi(n)} = 1 \bmod n$$

Proof: The multiplicative group $G = \mathbf{Z}/n^\times$ has $\varphi(n)$ elements. For $b \in G$, by Lagrange's theorem and the proposition that $|\langle g \rangle| = |g|$, the order ℓ of b divides the order $|G| = \varphi(n)$ of G, so write $\ell = N \cdot \varphi(n)$. Then

$$b^{\varphi(n)} = (b^\ell)^N = 1^N = 1 \bmod n$$

///

Rings

A **ring** R is a set with two binary operations $+$ and $*$ (addition and multiplication) with special element 0 such that

- R with $+$ and 0 is an abelian group
- $*$ is associative
- Distributivity: $a*(b+c) = a*b+a*c$ and $(b+c)*a = b*a+c*a$

If the multiplication is commutative, say the ring is **commutative**.

If there is an element $1 \in R$ such that $1*r = r*1 = r$ call this 1 a **multiplicative identity**. The 0 is the **additive identity**.

Example: The integers **Z** with the usual addition, multiplication, and 0 and 1 form a commutative ring.

As an example of a universally true assertion which transcends our usual intuition for multiplication as repeated addition:

Proposition: In any ring R, for all $r \in R$

$$0 * r = 0$$

Proof: We have

$$\begin{aligned} 0 * r &= (0 + 0) * r && \text{(property of 0)} \\ &= 0 * r + 0 * r && \text{(distributivity)} \end{aligned}$$

Add the additive inverse $s = -(0 * r)$ (whatever it may be!) to both sides

$$\begin{aligned} 0 &= s + (0 * r + 0 * r) && \text{(inverse prop)} \\ &= (s + 0 * r) + 0 * r && \text{(associativity)} \\ &= 0 + 0 * r && \text{(inverse property)} \\ &= 0 * r && \text{(identity property)} \end{aligned}$$

as claimed. ///

Another example, which gives a stronger explanation of the slogan *a minus times a minus is a plus:*

Proposition: In any ring R

$$(-r) * (-s) = r * s$$

Proof: First, claim that $-(-r) = r$. Using uniqueness of additive inverses in a group, check by adding, namely that $(-r) + r = 0$.

Next, claim that $-(r * s) = (-r) * s$. Using uniqueness of additive inverses, check by adding, using distributivity

$$r * s + (-s) * s = (r + (-r)) * s = 0 * s = 0$$

Then

$$\begin{gathered} -(r * s) + (-r) * (-s) \\ = (-r) * s + (-r) * (-s) \\ = (-r) * (s + (-s)) = (-r) * 0 = 0 \end{gathered}$$

This proves that $(-r) * (-s)$ is additive inverse of $-(r * s)$. But also $r * s$ is an additive inverse of $(-r * s)$, so by uniqueness of additive inverses

$$(-r) * (-s) = r * s$$

as claimed. ///