Crypto Theoretical Minimum
Groups and Finite Fields

Bassam El Khoury Seguias

BTC: 3FcVvBZwTUkUrcqJd16RcjR42qT2tDWHWn

ETH: 0xb79Fb9194C8Cc6221368bb70976e18609Ab9AcA8

May 18, 2018

1 Introduction

Group, field and elliptic curve theories make a regular appearance in the study of crypto-assets including but not limited to cryptocurrencies. For example, the security strength of a number of crypto-specific primitives relies on the math of elliptic curve groups over finite fields. These groups constitute a robust infrastructure to generate adequate public keys from private ones.

Groups and fields are foundational pillars of modern algebra. While in elementary algebra we rely on common arithmetic operations (e.g., addition and multiplication of real numbers), in modern algebra we raise further the level of abstraction. In particular, we introduce more general counterparts to real number addition and multiplication and define them over more general sets. An important objective is to study the common properties of all sets on which a fixed number of operations are defined. These operations tend to be interrelated in some definite way (e.g., distributivity of multiplication over addition).

In this post, we provide a concise (but by no means comprehensive) introduction to group and finite-field theory at the level needed to better appreciate the mathematical foundation of crypto assets. In a subequent post we build on this material to introduce elliptic curve groups defined over finite fields. The interested reader could consult e.g., [1] for a deeper dive on the theory of finite fields and its applications.

2 Groups - Axiomatic formulation

A group is a set G together with a binary operation $*$ on G such that $(G, *)$ satisfies the following properties:

1. *Associativity*: $a,\ b,\ c\ \in G\ \Rightarrow\ a * (b * c) = (a * b) * c$
2. *Existence of identity*: $\exists e \in G$ such that $\forall a \in G$, we have $a * e = e * a = a$

3. *Closure*: $a,\ b \in G\ \Rightarrow\ a * b \in G$

4. *Existence of inverse*: $\forall a \in G,\ \exists$ an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. We say that a^{-1} is the inverse of a in $(G, *)$

If in addition, the group satisfies the *commutativity* property: $a, b \in G\ \Rightarrow\ a*b = b*a$, the group $(G, *)$ is called **abelian**.

The aforementioned four axioms have an equivalent formulation in which the *closure* and *existence of inverse* properties get substitued with the *permutation* property. The axiomatic formulation becomes:

1. *Associativity*: $a,\ b,\ c\ \in G\ \Rightarrow\ a * (b * c) = (a * b) * c$

2. *Existence of identity*: $\exists e \in G$ such that $\forall a \in G$, we have $a * e = e * a = a$

5. *Permutation*: $\forall a \in G$, the set $a * G \equiv \{a * b \mid b \in G\}$ is a permutation of G

Proof (1, 2, 3 and 4 $\Rightarrow$ 5): For a fixed $a \in G$, consider the map

$$h_a : G \to a * G$$
$$h_a(g) = a * g$$

Proving that the *permutation* property holds is equivalent to showing that $\forall a \in G$, the map h_a is a bijection such that the domain G and the range $a * G$ are one and the same. To see this, note that $\forall a \in G$:

- $g \in G\ \Rightarrow a * g \in G$. (by the *closure* property). Hence $a * G \subset G$.
- h_a is surjective: This is clear from the definition of h_a since any element of its range is of the form $a * g$ for some $g \in G$ and hence admits g as a pre-image.
- h_a is injective: Suppose that $a * g_1 = a * g_2$, for some $g_1, g_2 \in G$. The *existence of inverse* property, coupled with the *associativity* property allow us to write

$$g_1 = (a^{-1} * a) * g_1 = a^{-1} * (a * g_1) = a^{-1} * (a * g_2) = (a^{-1} * a) * g_2 = g_2.$$

Proof (5 $\Rightarrow$ 3): If $a, b \in G$, then $(a * b) \in (a * G)$ by definition. Since the *permutation* property holds, then $a * G$ is a permutation of G and so $(a * b) \in G$. Consequently, the *closure* property holds.

Proof (1, 2, and 5 $\Rightarrow$ 4): If $a * G$ is a permutation of G, then by the *existence of identity* property it necessarily contains the identity element e of G. Consequently, $\exists g \in G$ such that $a * g = e$. In order to demonstrate that the *existence of inverse* property holds, we still have to show that $g * a = e$. To do so, consider the set $g * G$. By the *permutation* property, we know that $g * G$ is a permutation of G and so $\exists g' \in G$ such that $g * g' = e$. By invoking the *associativity* property, we can write

$$a = a * e = a * (g * g') = (a * g) * g' = e * g' = g' \text{ (Q.E.D.)}$$

The alternative axiomatic definition paves the way to a convenient representation of a group using a **Cayley table**. Let $G \equiv \{g_1, g_2, ..., g_n\}$. The Cayley table is simply:

$*$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\cdots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\cdots$	$g_2 * g_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$g_n * g_1$	$g_n * g_2$	$\cdots$	$g_n * g_n$

One can observe that the i^{th} row in the table above is none other than $g_i * G$ which corresponds to a specific permutation of G.

Uniqueness results

- The group identity element is unique. To see why, suppose there exists a group $(G, *)$ with two identity elements e and e'. By definition of e, it must be that $e' = e' * e$. Moreover, by definition of e', it must be that $e' * e = e$. As a result, we must have have $e' = e$.

- Similarly, the inverse of a group element is unique. To prove it, we make use of the *associativity* and *existence of inverse* properties. Let $a \in G$ and suppose that it admits two inverses i_1 and $i_2 \in G$. It must be that

$$a * i_1 \ = \ i_1 * a \ = \ a * i_2 \ = \ i_2 * a \ = \ e.$$

  And so we can write:

$$i_1 \ = \ i_1 * e \ = \ i_1 * (a * i_2) \ = \ (i_1 * a) * i_2 \ = \ e * i_2 \ = i_2$$

3 Group examples

Group examples abound. In this post, we limit ourselves to two examples of particular importance: the group of integers modulo n, and the group of powers of an

arbitrary element of some group. The importance of the former is partly derived from its role in building the canonical example of a finite field whenever n is a prime number (see section 8 below). Finite fields are of great significance in crypto in particular because the Discrete Logarithm (DL) problem is thought to be hard on their multiplicative subgroup. This intractability is at the heart of the security strength of a vast number of crypto primitives. The importance of the latter example comes from its crucial role in the study of cyclic groups, regularly used in the context of crypto.

Example 1: The group $(\mathbb{Z}_n, \oplus)$ of integers modulo n.

In order to define the group's underlying set and corresponding binary operation, we will need to introduce the notions of **equivalence relation**, **equivalence class**, and **modulo arithmetic**.

1. **Equivalence relation**: An equivalence relation on a set S is a subset $R \subset S \times S$ that satisfies three properties:
   (a) *Reflexivity*: $\forall s \in S, (s, s) \in R$
   (b) *Symmetry*: $(s, t) \in R \Rightarrow (t, s) \in R$
   (c) *Transitivity*: $(s, t), (t, u) \in R \Rightarrow (s, u) \in R$
2. **Equivalence class**: We let $[s]_R$ denote the set $\{t \in S \mid (s, t) \in R\}$ and refer to it as the equivalence class of the element $s \in S$ under the equivalence relation R. The set $\mathcal{E} \equiv \{[s]_R,\ s \in S\}$ of equivalence classes forms a partition of S. To see why, note the following:
   (a) $\mathcal{E}$ covers S: $\forall s \in S,\ (s, s) \in R$ (by the *reflexivity* property), hence $s \in [s]_R$. As a result, $\forall s \in S$, s belongs to at least one equivalence class.
   (b) Equivalence classes are disjoint:
   - let $[s]_R$ and $[t]_R$ be two equivalence classes on S that share an element $i \in S$ in common. Hence $(s, i) \in R$ and $(t, i) \in R$.
   - Let $f \neq i$ be any other element of $[t]_R$. Hence $(t, f) \in R$.
   - Since $(t, i) \in R$, then $(i, t) \in R$ (by the *symmetry* property). And since $(i, t) \in R$ and $(t, f) \in R$, then $(i, f) \in R$. (by the *transitivity* property).
   - We also know that $(s, i) \in R$. Using the *transitivity* property on (s, i) and (i, f), we conclude that $(s, f) \in R$. As a result, $f \in [s]_R$.

   Similarly, we can show that any element of $[s]_R$ is also an element of $[t]_R$.
3. **Modulo arithmetic**: One says that a positive integer a is congruent to another positive integer b modulo n if n divides $(a - b)$. An equivalent statement would be that a and b have the same remainder upon division by n. We denote this by $a \equiv b \pmod{n}$.

We are now in a position to define our first group example. Consider the set $\mathbb{Z}$ of integers. $\forall n \in \mathbb{Z}$, define a binary relation R_n on $\mathbb{Z} \times \mathbb{Z}$ as follows:

$$(a, b) \in R_n \iff a \equiv b \pmod{n}$$

One can easily see that R_n satisfies all three properties of an equivalence relation. We can therefore define equivalence classes on $\mathbb{Z}$ under the equivalence relation R_n. We denote by $[a] \equiv [a]_{R_n}$ the equivalence class of $a \in \mathbb{Z}$. By definition of R_n, we have:

$$[a] = \{a + kn \mid k \in \mathbb{Z}\} \equiv \{..., a - 2n, a - n, a, a + n, a + 2n, ...\}$$

Note that $[a]$ is equivalent to $[a + kn]$, for all $k \in \mathbb{Z}$. The equivalence classes associated with the equivalence relation R_n form a partition of $\mathbb{Z}$ and can be listed as follows:

$$\begin{gathered}
[0] \equiv \{..., -2n, -n, 0, n, 2n, ...\} \\
[1] \equiv \{..., -2n + 1, -n + 1, 1, n + 1, 2n + 1, ...\} \\
... \\
[n - 1] \equiv \{..., -n - 1, -1, n - 1, 2n - 1, 3n - 1, ...\}
\end{gathered}$$

We let $\mathbb{Z}_n \equiv \{[0], [1], ..., [n - 1]\}$, and define the binary operation $\oplus$ on a tuple $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ as follows:

$$[a] \oplus [b] = [a + b], \text{ where } + \text{ denotes regular addition of integers.}$$

This relationship does not depend on a particular element within a given equivalence class. Indeed, let $a + kn$ be any element of $[a]$ and $b + k'n$ any element of $[b]$, for $k, k' \in \mathbb{Z}$. Applying the binary relation on the equivalence classes $[a + kn]$ and $[b + k'n]$ yields:

$$[a + kn] \oplus [b + k'n] = [a + b + (k + k')n] = [a + b] = [a] + [b]$$

We claim that $(\mathbb{Z}_n, \oplus)$ is an abelian group. To prove this, we show that it satisfies the group axioms:

- *Associativity*: Let $[a], [b], [c] \in G$. We can write

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c]$$

$$= [a + (b + c)] = [(a + b) + c] \text{ (by associativity of } +)$$

$$= [a + b] \oplus [c] = ([a] \oplus [b]) \oplus [c]$$

- *Existence of identity*: Let $e \equiv [0]$. Clearly $e \in \mathbb{Z}_n$. Moreover, $\forall [a] \in \mathbb{Z}_n$, we have

$$[a] \oplus e = [a] \oplus [0] = [a + 0] = [a]$$

  Similarly, we can check that $e \oplus [a] = [a]$. Hence e satisfies the attributes of the identity element.

- *Closure*: Let $[a], [b] \in \mathbb{Z}_n$. By definition of $\oplus$, we have $[a] \oplus [b] = [a + b]$. And since the set $\mathbb{Z}_n \equiv \{[0], [1], ..., [n - 1]\}$ forms a partition of $\mathbb{Z}$, we can be confident that $[a + b]$ corresponds to exactly one element of this set and hence $[a + b] \in \mathbb{Z}_n$.

- *Existence of inverse*: $\forall [a] \in \mathbb{Z}_n$, we have $[a] \oplus [-a] = [a - a] = [0] = e$. Similarly,

we can conclude that $[-a] \oplus [a] = e$. Noting that $[-a] \in \mathbb{Z}_n$, this shows that each element of $\mathbb{Z}_n$ admits an inverse that is also an element of $\mathbb{Z}_n$.

- *Commutativity*: By definition of $\oplus$, we have

$$[a] \oplus [b] \;=\; [a+b] \;=\; [b+a] \;=\; [b] \oplus [a].$$

Example 2: The group of powers of an arbitrary element of some group

Let $(G, *)$ be a group and $a \in G$. Consider the set of all powers of a defined as

$$\{a\} \equiv \{a^i,\ i \in \mathbb{N}^*\}, \text{ where } a^i \equiv a * a * ... * a \ (i \text{ times})$$

We claim that $(\{a\}, *)$ is a group. To prove it, we show that $(\{a\}, *)$ satisfies the group axioms.

- *Associativity*: Let a^i, a^j and a^k be elements of $\{a\}$. We get the following equalities:

$$a^i * (a^j * a^k) = a^i * (a^{j+k}) = a^{i+(j+k)} \text{ (by definition of power)}$$

$$= a^{(i+j)+k} \text{ (by associativity of } +)$$

$$= a^{i+j} * a^k = (a^i * a^j) * a^k$$

- *Existence of identity*: Note that since G is finite, and since all powers of a are elements of G (because of the *closure* property of $(G, *)$), the powers of a cannot yield different elements ad infinitum. Consequently, there must exist a least integer n such that $a^n = a^i$ for some $1 \leq i < n$. We claim that the $(n-i)^{th}$ power of a, is the identity element of $\{a\}$. To see why, let a^r be any element of $\{a\}$. We can write

$$a^r * a^{n-i} = a^{r-i} * a^n \text{ (by definition of power)}$$

$$= a^{r-i} * a^i \text{ (since } a^n = a^i)$$

$$= a^r \text{ (by definition of power)}$$

  Similarly, we can show that $a^{n-i} * a^r = a^r$. Since a^r was arbitrary in $\{a\}$, we conclude that a^{n-i} satisfies the properties of an identity element.

- *Closure*: Let a^i, a^j be two elements of $\{a\}$. By the definition of power of a, we get $a^i * a^j = a^{i+j}$. This is clearly a power of a and therefore an element of $\{a\}$.

- *Existence of inverse*: Let a^r be an arbitrary element of $\{a\}$. Recall that the identity element of $\{a\}$ is equal to a^{n-i}. Since $i < n$, we can always find a least integer k such that $k(n-i) - r > 0$. We get:

$$a^{n-i} \;=\; e \;=\; e * e * ... * e \ (k \text{ times})$$

$$= a^{k(n-i)} = a^{k(n-i)+r-r} = a^r * a^{k(n-i)-r} = a^{k(n-i)-r} * a^r$$

Since $k(n-i)-r > 0$, we conclude that $a^{k(n-i)-r} \in \{a\}$ and qualifies as the inverse of a^r.

4 Subgroups, cosets and Lagrange's theorem

Given a group $(G, *)$ and a subset $H \subset G$, we say that $(H, *)$ a **subgroup** of $(G, *)$ if $(H, *)$ is a group. A subgroup is mandated to be a group with respect to the same operation of the parent group. A direct consequence is that the identity element of $(H, *)$ is the same as that of $(G, *)$. Clearly, the power group $\{a\}$ previously introduced, is a subgroup of $(G, *)$ for all $a \in G$.

If $(H, *)$ is a subgroup of $(G, *)$, one can define a relation on $G \times G$ as follows:

$$R_H : G \times G \longrightarrow \{1, 0\}$$

$$R_H(a, b) = 1 \iff \exists h \in H \text{ such that } b = a * h$$

R_H is an equivalence relation on $G \times G$ because it has all three desired properties:

1. *Reflexivity*: Let e denote the identity element of $(G, *)$. $\forall a \in G,\ a = a * e$. Since $(H, *)$ is a subgroup of $(G, *)$, e is also the identity element of $(H, *)$ and $e \in H$. Consequently,$R_H(a, a) = 1$.

2. *Symmetry*: Let $a, b \in G$ such that $R_H(a, b) = 1$. We know that $\exists h \in H$ such that $b = a * h$. Moreover, since $(H, *)$ is a subgroup, h must admit a unique inverse $h^{-1} \in H$. This implies that $b * h^{-1} = a$. Therefore, $R_H(b, a) = 1$.

3. *Transitivity*: Let $a, b, c \in G$ such that $R_H(a, b) = R_H(b, c) = 1$. We know that $\exists h_1, h_2 \in H$ such that $b = a * h_1$ and $c = b * h_2$. Consequently, $c = (a * h_1) * h_2$. By *associativity* of $*$ on G, we get $c = a * (h_1 * h_2)$. Since $(H, *)$ is a group, the closure property guarantees that $h_3 \equiv h_1 * h_2 \in h$. Hence $c = a * h_3$ with $h_3 \in H$, and so $R_H(a, c) = 1$.

The equivalence relation R_H on G induces a partition of G into non-empty equivalent classes called **left cosets** of G modulo H. For $a \in G$, we denote its corresponding equivalence class by:

$$[a] = a * H = \{a * h \mid h \in H\}$$

By virtue of being a group, $(G, *)$ satisfies the *permutation* property i.e., $\forall a \in G,\ a * G$ is a permutation of G. A direct consequence is that for any subset $S \subset G$, $a * S$ will also be a permutation of S. In particular, $a * H$ is a permutation of H. This shows that every left coset of G modulo H has the same cardinality as H. We now state and prove a foundational theorem of group theory known as **Lagrange's theorem**.

Lagrange's theorem The order of (i.e., the number of elements conained in) any subgroup $(H, *)$ of a group $(G, *)$ divides the order of $(G, *)$.

Proof: Consider the equivalence classes generated by the relation R_H as previously defined. The classes form a partition of G. Moreover, they all contain the same number of elements as H (as we just proved). We can then write:

$$\text{order}(G, *) = (\#\text{ of equivalence classes generated by } R_H) \times \text{order}(H, *). \text{ Q.E.D}$$

5 Cyclic groups

Cyclic groups play a fundamental role in in the construction of secure cryptographic primitives used in e.g., cryptocurrencies. For one thing, a generator of a cyclic group is usually used as a base point to build public keys out of private ones. But most importantly, the security of a number of crypto primitives relies on the presupposed intractability of the **Discrete Logarithm** problem (DL) on certain cyclic groups. These include e.g.,

- The multiplicative cyclic group of a finite field of large prime order
- An appropriately chosen cyclic subgroup of an elliptic curve group

We say that a group $(G, *)$ is cyclic if and only if it can be generated by at least one of its elements, called a **generator**. In other words:

$$\text{A group } (G, *) \text{ is } \textbf{cyclic} \iff \exists g \in G \text{ such that } G = \{g\}$$

In what follows, we state and prove relevant results about cyclic groups in general.

1. *Any group of prime order is cyclic and can be generated by any of its non-identity elements*

   Proof:

   - Let $(G, *)$ be a group and p a prime number such that $\text{order}(G, *) = p$
   - By Lagrange's theorem, the order of any subgroup of $(G, *)$ must divide p. As a result, the order of any subgroup of $(G, *)$ can either be equal to 1 or to p.
   - The singleton $\{e\}$ consisting of $(G, *)$'s identity element yields the subgroup $(\{e\}, *)$ whose order is equal to 1. It is called the trivial subgroup.
   - Any other subgroup of $(G, *)$ must be of order at least 2 because at a minimum, it must contain a non-identity element in addition to the identity.
   - Consequently, the order of any subgroup of $(G, *)$ other than the trivial subgroup $\{e\}$ must be equal to p.
   - In particular, the subgroups generated by each non-identity element must have an order equal to p. Therefore $\forall g \in G,\ g \neq e$, it must be that g is a generator of G, i.e., $G = \{g\}$. Q.E.D.

2. *Every subgroup of a cyclic group is cyclic*

   Proof:

   - Let $(G, *)$ be a cyclic group. Hence $\exists a \in G$ such that $G = \{a\}$. Let $(H, *)$ be a subgroup of $(G, *) \equiv (\{a\}, *)$.
   - Either $H = \{e\}$ or H contains at least one positive power of a. If $H = \{e\}$, then it is clearly cyclic. Otherwise, let d be the least positive exponent such that $a^d \in H$. We show that H is cyclic by demonstrating that $H = \{a^d\}$
   - By definition, we have the following equivalences:

   $$H = \{a^d\} \iff \forall h \in H,\ h = a^s \text{ where } a^s \text{ is a positive power of } a^d$$

   $$\iff \forall h \in H,\ h = a^s \text{ where } s \text{ is a positive mutiple of } d$$

   - Since H is a subset of $\{a\}$, anyone of its elements must be of the form a^s where s is a positive integer greater than or equal to d.
   - Suppose however that s is not a multiple of d. We can write $s = qd + r$ with $0 < r < d$ and $q \in \mathbb{N}^*$. This implies that $a^s = a^{qd+r} = (a^d)^q * a^r$.
   - By virtue of being an element of H, a^d admits an inverse $a^{-d} \in H$. The *closure* property implies that both $(a^d)^q$ and $(a^{-d})^q$ are elements of H. One can also easily verify that $(a^{-d})^q$ is the inverse of $(a^d)^q$. We then write:

   $$(a^{-d})^q * a^s = (a^{-d})^q * ((a^d)^q * a^r) = a^r$$

   - Noting that $(a^{-d})^q$ and a^s are both elements of H, we conclude that $a^r \in H$.
   - But $r < d$, being the remainder of the division of s by d. This contradicts the fact that d is the least positive integer such that $a^d \in H$. Consequently, we conclude that s must be a multiple of d.
   - Coupled with the fact that $\forall h \in H,\ h$ is of the form a^s for some positive integer s greater than or equal to d, we conclude that $H = \{a^d\}$. Q.E.D.

3. *In a finite cyclic group* $(\{a\}, *)$ *of order* m*, the element* a^k *generates a subgroup* $(\{a^k\}, *)$ *of order* $\frac{m}{gcd(k,m)}$

   Proof:

   - Let $d \equiv \gcd(k, m)$.
   - It is easy to see that the order of $(\{a^k\}, *)$ corresponds to the least integer n such that $(a^k)^n = e$ (where e is the identity element of the group). Similarly, m is the least integer that satisfies $a^m = e$.
   - We claim that $a^{kn} = e \iff m$ divides kn

     $\Leftarrow$: If m divides kn, then $kn = \alpha m$ for some integer α. Consequently, $a^{kn} = a^{\alpha m} = (a^m)^\alpha = e^\alpha = e$.

     $\Rightarrow$: Suppose $a^{kn} = e$, with kn not a multiple of m, i.e., $kn = qm + r$, where $0 < r < m$ and $q \in \mathbb{N}$. This implies $e = a^{kn} = a^{qm} * a^r = a^r$, a contradiction since m is the least integer that satisfies $a^m = e$.

- Next, we claim that m divides $kn \iff \frac{m}{d}$ divides n

  $\Rightarrow$: If m divides kn, then $\frac{m}{d}$ divides $\frac{kn}{d}$ (note that $\frac{m}{d}$ and $\frac{k}{d}$ are both integers since $d \equiv \gcd(k,m)$). Since $\gcd(\frac{k}{d}, \frac{m}{d}) = 1$, the integers $\frac{m}{d}$ and $\frac{k}{d} do not share a common divisor greater than 1$. But $\frac{m}{d}$ divides $\frac{kn}{d}$ and so it must be that $\frac{m}{d}$ divides n.

  $\Leftarrow$: If $\frac{m}{d}$ divides n, it must be that m divides dn. But $d = \gcd(k,m)$ and so d divides k. As a result, m divides kn.

- The previous two equivalences prove that

$$a^{kn} = e \iff \frac{m}{d} \text{ divides } n.$$

  Recall that n is the least integer that satisfies $a^{kn} = e$. The equivalence then dictates that n must be the least integer such that $\frac{m}{d}$ divides n. Consequently, it must be that $n = \frac{m}{d} = \frac{m}{gcd(k,m)}$. Q.E.D.

4. *In a finite cyclic group $(\{a\}, *)$ of order m, for any positive divisor f of m, $\{a\}$ contains one and only one subgroup of order f.*

   Proof:

   Existence: Consider the subgroup $(\{a^{\frac{m}{f}}\}, *)$ generated by the element $a^{\frac{m}{f}} \in \{a\}$ (note that $\frac{m}{f}$ is an integer since f is a divisor of m). By result #3 above, the order of $(\{a^{\frac{m}{f}}\}, *)$ must be equal to $\frac{m}{gcd(\frac{m}{f},m)}$ which is equal to $\frac{m}{\frac{m}{f}} = f$. This shows that $(\{a\},*)$ admits at least one subgroup of order f.

   Uniqueness:

   - Suppose that $(\{a\},*)$ has another subgroup of order f. By result #2 above, every subgroup of a cyclic group is cyclic. Therefore, this other subgroup of order f must be cyclic and hence generated by a certain power a^i of a.
   - By result #3 above, it must be that $f = \text{order}(\{a^i\}, *) = \frac{m}{gcd(i,m)}$. Consequently, $\frac{m}{f} = \gcd(i,m)$.
   - This shows that $\frac{m}{f}$ divides i, which allows us to write $i = q(\frac{m}{f})$ for some $q \in \mathbb{Z}$. And so $a^i = a^{q(\frac{m}{f})} = (a^{\frac{m}{f}})^q \in \{a^{\frac{m}{f}}\}$.
   - Since $a^i \in \{a^{\frac{m}{f}}\}$, we conclude that $(\{a^i\}, *)$ is a subgroup of $(\{a^{\frac{m}{f}}\}, *)$. But recall that $(\{a^i\}, *)$ and $(\{a^{\frac{m}{f}}\}, *)$ have the same order, and so they must be the same group. Q.E.D.

5. *Let $(\{a\}, *)$ be a finite cyclic group of order m, and f a divisor of m. Then $\{a\}$ contains $\phi(f)$ elements of order f. Moreover, $m = \sum_{f \mid f \text{ divides } m} \phi(f)$.*

   Note 1: The order of an element of a group is the order of the subgroup generated by that element.

   Note 2: $\phi(f)$ denotes the Euler's totient function applied to f which evaluates to the number of integers $1 \leq i \leq f$ that are relatively prime to f (i.e., integers i that satisfy $\gcd(i,f) = 1$).

Proof:

- Recall that result #3 stated that in a finite cyclic group $(\{a\}, *)$ of order m, the element a^k generates a subgroup $(\{a^k\}, *)$ of order $\frac{m}{gcd(k,m)}$.
- Therefore, if we're given an integer d that divides m, one can identify the integers $1 \leq k \leq m$ such that $\gcd(k, m) = d$, and conclude that each a^k generates a subgroup $(\{a^k\}, *)$ of order equal to $\frac{m}{d}$. This implies that the total count of such k's corresponds to the number of elements in $\{a\}$ that generate a subgroup of order $\frac{m}{d}$.
- Since f divides m, let $d = \frac{m}{f}$ so that $f = \frac{m}{d}$. As a result, the number of elements in $\{a\}$ that generate a subgroup of order f is equal to the number of integers $1 \leq k \leq m$ such that $\gcd(k, m) = d = \frac{m}{f}$.
- $\forall k$, we know that k is a multiple of $\gcd(k, m) = \frac{m}{f}$. In particular, for each valid k we can write $k = q(\frac{m}{f})$, where $q \in \mathbb{N}$ and $1 \leq k = q(\frac{m}{f}) \leq m$. As a result, the number of elements in $\{a\}$ that generate a subgroup of order f is equal to the number of integers of the form $q(\frac{m}{f})$ such that $1 \leq q(\frac{m}{f}) \leq m$ and $\gcd(q(\frac{m}{f}), m) = \frac{m}{f}$.
- Next, note the following equivalences:

$$\gcd(q(\tfrac{m}{f}), m) = \tfrac{m}{f} \iff \gcd(q(\tfrac{m}{f}), f(\tfrac{m}{f})) = \tfrac{m}{f} \iff \gcd(q, f) = 1$$

  We then conclude that the eligible integers of the form $q(\frac{m}{f})$ are those that correspond to integers $\frac{f}{m} \leq 1 \leq q \leq f$ such that q is coprime to f. This is none other that $\phi(f)$.
- Finally, by result #4 above, we know that in a finite cyclic group of order m, there exists one and only one subgroup of order f for every divisor f of m. Moreover, each element of the cyclic group belongs to one and only one subgroup. Consequently, $m = \sum_{f \mid f \text{ divides } m} \phi(f)$. Q.E.D.

6. *A finite cyclic group $(\{a\}, *)$ of order m contains $\phi(m)$ generators. The generators, are the powers a^q of a such that $gcd(q, m) = 1$*

   Proof: This is a special case of result #5 above, applied when $f = m$.

6 Group isomorphism

When comparing the structures of two groups, the mappings between them that preserve their respective operations take on an important role.

Given groups $(G, *)$ and $(H, \triangle)$, a mapping $f : G \longrightarrow H$ is called a **homomorphism** of G into H if it preserves the operation of $(G, *)$. That is:

$$a, b \in G \Rightarrow f(a * b) = f(a) \triangle f(b)$$

In the context of crypto, an important application of group homomorphism takes the form of a Pedersen Commitment. In Monero for example, Pederson Commitments are

used to hide the value of a transaction (refer to Part 8 of the Monero series for a detailed explanation).

If f is also bijective, then it is called an **isomorphism**. In this case, $(G, *)$ and $(H, \triangle)$ can be thought of as equivalent. Group isomorphisms are a special instance of the more general theory of categories and functors. The objective of the theory is to elucidate structural similarities that exist between various areas of mathematics. On a more subjective note, it may be one of the most beautiful theories of mathematics. For a very concise yet clear introduction, the interested reader may consult section 10 of [2].

7 Fields - Axiomatic formulation

Fields are algebraic structures that generalize arithmetics that we are used to on $\mathbb{R}$. More specifically, a field is a set endowed with the notions of **addition** and **multiplication** as well as with their respective inverses **subtraction** and **division**.

Formally, a field is a set $\mathbb{F}$ with at least two elements and two binary operations $\oplus$ and $\otimes$ such that:

1. $(\mathbb{F}, \oplus)$ is an abelian group. We denote its identity element by $\mathbf{0}$.
2. $(\mathbb{F}, \otimes)$ satisfies the 1)*Associativity*, 2) *Existence of identity*, 3) *Closure*, and 5) *Commutativity* group axioms. However, $(\mathbb{F}, \otimes)$ is not a group since the *Existence of inverse* axiom is not observed for all elements of $\mathbb{F}$. More specifically, the additive identity element $\mathbf{0}$ is not required to admit a multiplicative inverse.
3. $(\mathbb{F}^*, \otimes) \equiv (\mathbb{F} - \mathbf{0}, \otimes)$ is an abelian group. This means that by removing the additive identity element $\mathbf{0}$, the resulting set becomes an abelian group under multiplication. We denote its identity element by $\mathbb{1}$. This group is known as the field's **multiplicative** group (it turns out that it is also cyclic, but we will not prove it in this post).
4. *Distributivity of* $\otimes$ *over* $\oplus$: $\forall a, b, c \in \mathbb{F}$, we have $(a \oplus b) \ \otimes \ c = (a \otimes c) \ \oplus \ (b \otimes c)$

It is common to refer to $\oplus$ as the field's addition and to $\otimes$ as the field's multiplication. One implication of the aforementioned axioms is that $\forall a \in \mathbb{F}, \ a \otimes \mathbf{0} = \mathbf{0}$. To see this, note the following:

$$a \ = \ a \otimes \mathbb{1} \ = \ a \otimes (\mathbf{0} \oplus \mathbb{1}) \ = \ (a \otimes \mathbf{0}) \oplus (a \otimes \mathbb{1}) \ = \ (a \otimes \mathbf{0}) \oplus a$$

Being an element of $\mathbb{F}$, a admits an additive inverse (i.e., with respet to $\oplus$). As a result of cancelling a from each side of the above equality, we get $\mathbf{0} = a \otimes \mathbf{0}$.

The order of $\mathbb{F}$ is the number of elements that it contains. $\mathbb{F}$ is called a **finite field** if its order is finite. The theory of finite fields is rich and beautiful. One of its most important results states that finite fields can only have orders of the form p^m, where p is any prime number and m any positive integer. Moreover, it turns out that all fields that contain the same number of elements are equivalent.

To understand and better appreciate the canonical example of a finite field of order p^m, one will need to study prime polynomials over finite fields, which is out of scope. Nevertheless, we will introduce the case of $m = 1$ corresponding to the most basic type of a finite field, namely the field $\mathbb{F}_p$. It is the canonical example of finite fields of prime order p.

8 The field $\mathbb{F}_p$ of integers modulo p

Let $\mathbb{Z}_n$ and $\oplus$ be as defined in section 3 when we introduced the abelian group $(\mathbb{Z}_n, \oplus)$ of integers modulo n. Recall that

- $\mathbb{Z}_n \equiv \{[0],\ [1],\ ...,\ [n-1]\}$, where $[a] \equiv \{a + kn \mid k \in \mathbb{Z}\}$, and
- $\oplus$ is defined on $\mathbb{Z}_n \times \mathbb{Z}_n$ to be $[a] \oplus [b] \ = \ [a + b]$, where $+$ denotes regular addition of integers.

We introduce a multiplicative operation on $\mathbb{Z}_n \times \mathbb{Z}_n$ denoted by $\otimes$ and defined as follows:

$\forall [a], [b] \in \mathbb{Z}_n,\ [a] \otimes [b] \ = \ [a \times b]$, where $\times$ denotes regular multiplication of integers.

Note that this relationship does not depend on a particular element within a class. Indeed, let $a + kn$ be any element of $[a]$ and $b + k'n$ any element of $[b]$, for $k, k' \in \mathbb{Z}$. Applying the binary relation on the equivalence classes $[a + kn]$ and $[b + k'n]$ yields:

$$[a + kn] \otimes [b + k'n] \ = \ [ab + ak'n + bkn + kk'n^2]$$

$$= [ab + (ak' + bk + kk'n)n)] \ = \ [a \times b] \ = \ [a] \otimes [b]$$

We claim that $(\mathbb{Z}_n, \oplus, \otimes)$ **is a field if and only if** n **is prime**.

$\Rightarrow$: Suppose n were not prime. We will show that $(\mathbb{Z}_n^*, \otimes)$ would fail to satisy the *closure* axiom and as a result, would not be a group. Indeed, since n is composite, we can write $n = a \times b,\ 1 < a, b < n$. Clearly, $[a]$ and $[b]$ are elements of $\mathbb{Z}_n^*$. However,

$$[a] \otimes [b] = [a \times b] = [n] = [0] \equiv \mathbf{0} \notin \mathbb{Z}_n^*. \text{ Q.E.D.}$$

$\Leftarrow$: Let $n = p$ where p is a prime number. We have:

$(\mathbb{Z}_p, \oplus)$ **is an abelian group**: We previously proved in section 3 that this result holds for any positive integer n, and so holds true in particular when $n = p$ is a prime. Its identity element is $[0] \equiv \mathbf{0}$

$(\mathbb{Z}_p, \otimes)$ **satisfies the 1)** ***Associativity*****, 2)** ***Existence of identity*****, 3)** ***Closure*****, and 5)** ***Commutativity*** **group axioms**:

- *Associativity*: Let $[a], [b], [c] \in \mathbb{Z}_p$ and notice that:

$$[a] \otimes ([b] \otimes [c]) \ = \ [a] \otimes [b \times c] \ = \ [a \times (b \times c)]$$

$$= \ [(a \times b) \times c] \ = \ [a \times b] \otimes [c] \ = \ ([a] \otimes [b]) \otimes [c] \text{ Q.E.D.}$$

- *Existence of identity*: We claim that $[1]$ is the identity element. Clearly, $[1] \in \mathbb{Z}_p$. Moreover, $\forall a \in \mathbb{Z}_p$ we have

$$[a] \otimes [1] = [a \times 1] = [a], \text{ and } [1] \otimes [a] = [1 \times a] = [a] \text{ Q.E.D.}$$

- *Closure*: Let $[a], [b] \in \mathbb{Z}_p$. By definition of $\otimes$, we have $[a] \otimes [b] = [a \times b]$. And since the set $\mathbb{Z}_p \equiv \{[0],\ [1],\ ...,\ [p-1]\}$ forms a partition of $\mathbb{Z}$, we can be confident that $[a \times b]$ corresponds to exactly one element of this set and hence $[a \times b] \in \mathbb{Z}_p$. Q.E.D.

- *Commutativity*: $\forall [a], [b] \in \mathbb{Z}_p$, we can use the commutativity of regular multiplication on integers to conclude that

$$[a] \otimes [b] \ = \ [a \times b] \ = \ [b \times a] \ = \ [b] \otimes [a]. \text{ Q.E.D.}$$

$(\mathbb{Z}_p^*, \otimes)$ **is an abelian group**. We prove that it satisfies all five group axioms:

- *Associativity*: We previously proved associativity in $\mathbb{Z}_p$, which automatically implies associativity in $\mathbb{Z}_p^*$

- *Existence of identity*: We previously showed that $[1]$ is the identity element in $\mathbb{Z}_p$. This also implies that $[1]$ is the identity element in $\mathbb{Z}_p^*$

- *Closure*: Let $[a], [b] \in \mathbb{Z}_p^*$. Since p is prime, then $\forall\ 0 < a, b < p,\ a \times b \not\equiv 0 \pmod{p}$. If this were not true, one would be able to write $a \times b = kp$ for some positive integer k. And since p is prime, it must be that boh a and b divide k. Hence $a \times b$ divides k, implying that $k \geq a \times b$. This results in kp being strictly greater than $a \times b$, a contradiction. Consequently $[a] \otimes [b] \ = \ [a \times b] \ \neq \ [0]$ and so $[a] \otimes [b] \in \mathbb{Z}_p^*$. Q.E.D.

- *Existence of inverse*: Our purpose is to show that $\forall [a] \in \mathbb{Z}_p^*,\ \exists [x] \in \mathbb{Z}_p^*$ such that $[a] \otimes [x] = [x] \otimes [a] = \mathbb{1} \equiv [1]$. Note that $[a] \otimes [x] = [1]$ is equivalent to $[a \times x] = [1]$, which in turn is equivalent to $ax \equiv 1 \pmod{p}$. It turns out that when a and p are relatively prime, such an x always exists. To prove this, we make use of the following theorem

  Theorem: Given $a, b \in \mathbb{Z},\ g = gcd(a, b),\ \exists x, y \in \mathbb{Z}$ *such that* $ax + by = g$.

  A corollary to the theorem is that if a and b are relatively prime, then one can find integers x and y such that $ax + by = 1$. In our case, we know that a and p are relatively prime because p is prime and $a < p$. As a result, the theorem leads us to conclude that $\exists x$ such that $ax \equiv 1 \pmod{p}$. This in turn, proves that $[a]$ admits an inverse equal to $[x]$.

  Proof:

  { Since $a < p$, we can write $p = aq + r_1$ with $0 \leq r_1 < a$.

- { Next, note that $\gcd(p, a) = \gcd(a, r_1)$. To see this, observe that $\gcd(p, a)$ divides p and a and hence must divide $r_1 = p - aq$. As a result, $\gcd(p, a)$ must divide $\gcd(a, r_1)$. Similarly, $\gcd(a, r_1)$ divides a and r_1 and hence must divide $p = aq + r_1$ As a result, $\gcd(a, r_1)$ must divide $\gcd(p, a)$. Hence $\gcd(p, a)$ =$\gcd(a, r_1)$.
- { So instead of finding $\gcd(p, a)$, one can find $\gcd(a, r_1)$. We now write $a = r_1q_1 + r_2$ with $0 \leq r_2 < r_1$, and conclude that $\gcd(a, r_1) = \gcd(r_1, r_2)$.
- { Repeating the above step and noting that the remainder is always a non-negative integer strictly less than the divisor, we eventually reach the case where $r_n = 0$ after n iterations. And so we get

$$\gcd(p, a) = \gcd(a, r_1) = \gcd(r_1, r_2) = ... = \gcd(r_{n-1}, 0) = r_{n-1}$$

- { Noting that $r_{i+2} = r_i - r_{i+1}q_{i+1}$ is a linear combination of r_i and r_{i+1}, and that $r_1 = p - aq$ is a linear combination of p and a, we conclude that $g \equiv \gcd(p, a) = r_{n-1}$ is itself a linear combination of p and a. (One can conduct a back-substitution process to find the values of the coefficients, also known as **Bézout coefficients**). Hence $g = ax + by$ and $[a]$ admits an inverse in $\mathbb{Z}_n^*$ equals to $[x]$. Q.E.D.

- *Commutativity*: We previously proved commutativity in $\mathbb{Z}_p$, which automatically implies commutativity in $\mathbb{Z}_p^*$

Distributivity of $\otimes$ over $\oplus$: let $[a], [b], [c] \in \mathbb{Z}_p^*$. Then

$$[a] \otimes ([b] \oplus [c]) \;=\; [a] \otimes [b + c] \;=\; [a \times (b + c)]$$

$$= [a \times b \;+\; a \times c] \;=\; [a \times b] \oplus [a \times c] \;=\; ([a] \otimes [b]) \;\oplus\; ([a] \otimes [c]).$$ Q.E.D.

References

[1] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1986.

[2] L. W. Tu. *An Introduction to Manifolds.* Springer, 2010.