Algebra and RSA

Emil Straschil

ETH Zurich

2025

Algebra

- An **Algebra** is a *carrier set* A together with some *operations* $\sigma_1, \sigma_2, \ldots$
- We write $\langle A; \sigma \rangle$

Monoid

A **Monoid** is an Algebra $\langle A; \sigma \rangle$ where:

- The operation σ is **associative**
- There is a **neutral element** e

Associativity

Needs to satisfy $(a\ \sigma\ b)\ \sigma\ c = a\ \sigma\ (b\ \sigma\ c)$

Neutral Element

Needs to satisfy $e\ \sigma\ a = a\ \sigma\ e = a$ for all $a \in A$

Group

A **Group** is a Monoid where additionally there is an **inverse** element for each element.

Inverse

For a is an element $\hat{a}$ which satisfies $a \, \sigma \, \hat{a} = \hat{a} \, \sigma \, a = e$

Abelian Group

The group operation does not need to be commutative. A commutative Group is called **abelian**.

Examples

- $\langle \mathbb{N}; +, 0 \rangle$ is a Monoid, but not a Group
- $\langle \mathbb{Z}_m; +_m, 0 \rangle$ is a Group with the elements $\{0, 1, 2, \ldots, m-1\}$ and addition modulo m.

Subgroups

A **Subgroup**H of a Group G is a subset of G with the same operations as G. It has to be **closed**, meaning:

- $a * b \in H$ for all $a, b \in H$
- $e \in H$
- $\hat{a} \in H$ for $a \in H$

Homomorphisms

For two Groups $\langle G; *, \widehat{\ }, e \rangle$ and $\langle H; \star, \widetilde{\ }, e' \rangle$ a **Group Homomorphism** is a function $\varphi : G \to H$ which satisfies the *homomorphism property*.

Homomorphism Property

$$\varphi(a * b) = \varphi(a) \star \varphi(b)$$

If φ is a bijection we call it **Isomorphism** and write $G \simeq H$ ("G isomorph to H").

Homomorphism Commutes

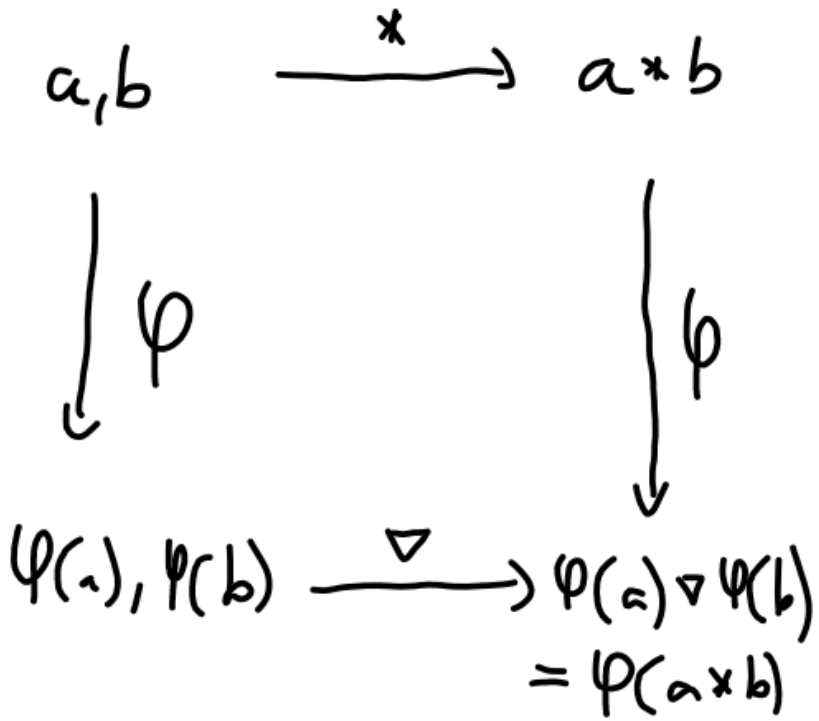


Figure: Commutative Homomorphism Square

Homomorphism Facts

For a homomorphism it holds that:

- $\varphi(e) = e'$
- $\widetilde{\varphi(a)} = \varphi(\widehat{a})$

And if $G \simeq H$ then they are *basically the same*. So we can work in G or H and then simply convert back and forth.

Order

Say we take an element of a Group and start operating on itself: $a^1, a^2, a^3, \ldots$ The power k at which $a^k = e$ for the first time is called the **order** of a ($ord(a)$).
Example: In $\mathbb{Z}_8$ the $ord(2) = 4$ since $2^4 = 0$

Lagrange

For a finite Group G and any $a \in G$ the order of a divides $|G|$

Cyclic Groups

A group is **cyclic** if it is *generated* by some **generator**. Example: $\mathbb{Z}_{10}$ is a cyclic group. It is generated by the element 1. The element 2 generates the subgroup $\{0, 2, 4, 6, 8\}$

Consequences from Lagrange

Prime Order Groups

Any Group G of prime order is cyclic.

Proof: Take any $a \neq e$ in G. Then $ord(a)$ divides $|G|$, but since $|G|$ is prime $ord(a) = |G|$. This means that a generates G and therefore G is cyclic.

Prime Order Generators

In a Group of prime order any non-neutral element is a generator of the group.

Proof: Since above a was arbitrary this holds for all $a \in G$.

Isomorphisms

Cool Theorem

Any cyclic group G is isomorph to $\mathbb{Z}_{|G|}$. (This implies that it is abelian.)

Exercise: Calculate $7^{123} * 7^{52}$ using a known isomorphism.

Isomorphisms

Cool Theorem

Any cyclic group G is isomorph to $\mathbb{Z}_{|G|}$. (This implies that it is abelian.)

Exercise: Calculate $7^{123} * 7^{52}$ using a known isomorphism.

Solution: Using the isomporphism from $\mathbb{Z}$ to $\{2^x | x \in \mathbb{Z}\}$ we get 7^{175}

Eulers Totient

Eulers Totient

$$\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$$

where $p_i^{e_i}$ are the prime factors of m.

Meaning: $\varphi(m)$ gives us the amount of numbers $x < m$ such that $gcd(x, m) = 1$ (x coprime to m).

Prime Eulers Totient

$\varphi(p) = p - 1$ for p prime.

Calculating Eulers Totient

Looks complicated? Let's do an example: Calculate $\varphi(504)$.
Step 1: Prime Factors We find that $504 = 2^3 * 3^2 * 7$.

Calculating Eulers Totient

Looks complicated? Let's do an example: Calculate $\varphi(504)$.
Step 1: Prime Factors We find that $504 = 2^3 * 3^2 * 7$.
Step 2: Adjust We subtract 1 from each power, giving us $(1 * 2^2) * (2 * 3^1) * (6)$.

Calculating Eulers Totient

Looks complicated? Let's do an example: Calculate $\varphi(504)$.
Step 1: Prime Factors We find that $504 = 2^3 * 3^2 * 7$.
Step 2: Adjust We subtract 1 from each power, giving us $(1 * 2^2) * (2 * 3^1) * (6)$.
Step 3: Calculate We find that $\varphi(504) = 144$

Eulers Totient Facts

Multiplicative Group Modulo m

$\varphi(m) = |\mathbb{Z}_m^*|$

Useful Fact

$\varphi(m)$ is the amount of generators of the group $\mathbb{Z}_m$.

Very Useful Fact

$a^{\varphi(m)} \equiv_m 1$ for $m \geq 2$ and $gcd(a, m) = 1$

Diffie-Hellman

One-Way Function

A one-way function is a function that is feasible to compute, but infeasible to reverse. This means we can compute $f(x)$ for some x, but not $f^{-1}(y) = x$ for some $y = f(x)$.

Modulo Exponentiation

$x \mapsto R_p(g^x)$ for a prime p is a one-way function.

Diffie-Hellman

1. Choose prime p and basis g (both are public).

Diffie-Hellman

1. Choose prime p and basis g (both are public). **2.** Alice and Bob choose a and b and calculate $y_a = R_p(g^a)$ and $y_b = R_p(g^b)$ (a and b are secret).

Diffie-Hellman

1. Choose prime p and basis g (both are public). **2.** Alice and Bob choose a and b and calculate $y_a = R_p(g^a)$ and $y_b = R_p(g^b)$ (a and b are secret). **3.** Send y_a and y_b to each other (now public).

Diffie-Hellman

1. Choose prime p and basis g (both are public). **2.** Alice and Bob choose a and b and calculate $y_a = R_p(g^a)$ and $y_b = R_p(g^b)$ (a and b are secret). **3.** Send y_a and y_b to each other (now public). **4.** Calculate $k = (y_b)^a = (y_a)^b$.

Diffie-Hellman

The result is:

1. Alice and Bob have the **same** value k.
2. Attacker only knows p, g, and y_a, y_b.

We cannot calculate k or a or b from those values alone!

Diffie-Hellman vs. RSA

Diffie-Hellman: We want to agree on a shared value k. We cannot choose that value, but we will get the same one and no one else can see it.

Diffie-Hellman vs. RSA

Diffie-Hellman: We want to agree on a shared value k. We cannot choose that value, but we will get the same one and no one else can see it.

RSA: Bob wants to send Alice some secret value. Alice gives Bob a "box" (matematical function) that only Alice can "open" (compute the value). Bob "puts his value into the Box" (encrypts it with the function), sends it to Alice, which "opens" it (decrypts it) and sees the value Bob sent her.

RSA Prerequisites

Roots

For G finite and $e \in \mathbb{Z}$ with $gcd(|G|, e) = 1$ the function $x \mapsto x^e$ is a bijection. The *e-th root of y* is x which satisfies $x^e = y$.

Finding Roots

We can find such an *e-th root* $x \in G$ for $y \in G$ with

$$x = y^d$$

where

$$ed \equiv_{|G|} 1$$

RSA Prerequisites

Prime Stuff

For $n = pq$ for p and q being large primes, one cannot compute $\varphi(n) = (p-1)(q-1)$ without knowing p and q. (At least not feasibly.)

Basis of RSA

When $|G|$ is known we can easily compute d such that $ed \equiv_{|G|} 1$ with the *extended Euclid algorithm.*

Basis of RSA

When $|G|$ is known we can easily compute d such that $ed \equiv_{|G|} 1$ with the *extended Euclid algorithm.*
How? Extended Euclid gives us λ, μ such that $\lambda e + \mu |G| = 1$ (since e and $|G|$ are coprime. Now $\lambda e \equiv_{|G|} 1$ which means choosing $d = \lambda$ is our inverse.

Basis of RSA

When $|G|$ is known we can easily compute d such that $ed \equiv_{|G|} 1$ with the *extended Euclid algorithm.*
How? Extended Euclid gives us λ, μ such that $\lambda e + \mu |G| = 1$ (since e and $|G|$ are coprime. Now $\lambda e \equiv_{|G|} 1$ which means choosing $d = \lambda$ is our inverse.
BUT if the group order $|G|$ is not known, it is not possible to compute d.

Basis of RSA

When $|G|$ is known we can easily compute d such that $ed \equiv_{|G|} 1$ with the *extended Euclid algorithm.*
How? Extended Euclid gives us λ, μ such that $\lambda e + \mu |G| = 1$ (since e and $|G|$ are coprime. Now $\lambda e \equiv_{|G|} 1$ which means choosing $d = \lambda$ is our inverse.
BUT if the group order $|G|$ is not known, it is not possible to compute d.
We exploit this to create a one-way function: One can easily compute x^e without knowing the group order, but only we know d to find the root x again.

RSA

1. We work in the group $\mathbb{Z}_n^*$

RSA

1. We work in the group $\mathbb{Z}_n^*$
2. Alice generates two primes p and q

RSA

1. We work in the group $\mathbb{Z}_n^*$
2. Alice generates two primes p and q
3. Alice calculates $n = pq$ (modulo we work in)

RSA

1. We work in the group $\mathbb{Z}_n^*$
2. Alice generates two primes p and q
3. Alice calculates $n = pq$ (modulo we work in)
4. Alice calculates $f = (p-1)(q-1) = \varphi(n) = |\mathbb{Z}_n^*|$

RSA

1. We work in the group $\mathbb{Z}_n^*$
2. Alice generates two primes p and q
3. Alice calculates $n = pq$ (modulo we work in)
4. Alice calculates $f = (p-1)(q-1) = \varphi(n) = |\mathbb{Z}_n^*|$
5. Alice selects e, calculates d with $ed \equiv_f 1$

RSA

1. We work in the group $\mathbb{Z}_n^*$
2. Alice generates two primes p and q
3. Alice calculates $n = pq$ (modulo we work in)
4. Alice calculates $f = (p-1)(q-1) = \varphi(n) = |\mathbb{Z}_n^*|$
5. Alice selects e, calculates d with $ed \equiv_f 1$
6. Alice sends (n, e) to Bob

RSA

Ok, let's recap this.

RSA

Ok, let's recap this. **Alice** now knows d, which means if someone sends her some $x^e = y$ she can calculate $x = y^d = x^{ed} = x^1$ from that.

RSA

Ok, let's recap this. **Alice** now knows d, which means if someone sends her some $x^e = y$ she can calculate $x = y^d = x^{ed} = x^1$ from that.
Publicly known are only n and e. Note that this is enough to calculate x^e in the group $\mathbb{Z}_n^*$. We don't need to know the group *order* for this! Only n is enough.

RSA

Ok, let's recap this. **Alice** now knows d, which means if someone sends her some $x^e = y$ she can calculate $x = y^d = x^{ed} = x^1$ from that.
Publicly known are only n and e. Note that this is enough to calculate x^e in the group $\mathbb{Z}_n^*$. We don't need to know the group *order* for this! Only n is enough.
But since f is not known, no one (other than Alice) can compute d. Remember that we cannot compute $f = \varphi(n)$ without knowing p and q (and only Alice knows those).

RSA

So now:

1. Bob has his secret value $m < n$
2. Bob calculates $c = R_n(m^e)$
3. Bob sends that to Alice
4. Alice calculates $R_n(c^d) = R_n(m^{ed}) = R_n(m^1) = m$

RSA

So now:

1. Bob has his secret value $m < n$
2. Bob calculates $c = R_n(m^e)$
3. Bob sends that to Alice
4. Alice calculates $R_n(c^d) = R_n(m^{ed}) = R_n(m^1) = m$

Bob can easily compute his c, since he knows e and n, but no one other than Alice knows d, so only she can decrypt it to obtain m again.

Attacking RSA

Assume Alice is not very smart and chooses small primes p and q. Then an attacker could simply guess $pq = n$ and then calculate f. Knowing f, one can then use Euclid just as Alice did to obtain d and decrypt the message.

Rings

A **Ring** is an algebra $\langle R; +, -, 0, *, 1 \rangle$ which satisfies three properties:

- $\langle R; +, -, 0 \rangle$ is a commutative group
- $\langle R; *, 1 \rangle$ is a monoid
- $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

Example: $\mathbb{Z}$ is a ring

Unit

We call elements a of a ring which have an inverse a^{-1} **units**. R^* is the multiplicative group of units in R.

Ring Exercises

9.4 Elementary Properties of Rings ($\star\,\star$)

The goal of this exercise is to prove Lemma 5.17 (ii) and (iii). You can use only Lemma 5.17 (i), which is proved in the lecture notes. In Subtask b), you can use Subtask a).

Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring and let $a, b \in R$. Show that:

a) $(-a)b = -(ab)$

b) $(-a)(-b) = ab$

Ring Exercises

9.4 Elementary Properties of Rings

a) We have

$$(-a)b + ab \overset{\text{distrib.}}{=} (-a+a)b \overset{\text{def. inverse}}{=} 0b \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Therefore, $(-a)b$ is the additive inverse of ab, which means that $(-a)b = -ab$.

b) We have

$$(-a)(-b) + (-(ab)) \overset{\text{a)}}{=} (-a)(-b) + (-a)b \overset{\text{distrib.}}{=} (-a)(-b+b)$$
$$\overset{\text{def. inverse}}{=} (-a)0 \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Therefore, $(-a)(-b)$ is the additive inverse of $-(ab)$, which means that $(-a)(-b) = -(-(ab)) = ab$.

Ring Exercises

Almost Ring

Take an Algebra which satisifes all the properties of Def. 5.18, except commutativity:

- $\langle R; +, -, 0 \rangle$ is a group
- $\langle R; *, 1 \rangle$ is a monoid
- distributivity holds

Prove that the addition in this algebra is commutative, so $a + b = b + a$.
Hint: Consider $(1 + 1)(a + b)$.

Ring Exercises

9.4 Non Minimality of Ring Axioms

We only need to show that the operation $+$ is commutative. Let $a, b \in R$.
We have

$$\begin{aligned}
(1+1)(a+b) &= (1+1)a + (1+1)b && \text{(Axiom iii), distributivity)} \\
&= (1a+1a) + (1b+1b) && \text{(Axiom iii), distributivity, twice)} \\
&= (a+a) + (b+b) && \text{(Axiom ii), neutral element)} \\
&= a+a+b+b && \text{(Axiom i), associativity)}
\end{aligned}$$

But also

$$\begin{aligned}
(1+1)(a+b) &= 1(a+b) + 1(a+b) && \text{(Axiom iii), distributivity)} \\
&= (1a+1b) + (1a+1b) && \text{(Axiom iii), distributivity, twice)} \\
&= (a+b) + (a+b) && \text{(Axiom ii), neutral element)} \\
&= a+b+a+b && \text{(Axiom i), associativity)}
\end{aligned}$$

Therefore

$$\begin{aligned}
& a+b+a+b = a+a+b+b \\
\overset{\cdot}{\iff} & a+b+a+b+(-b) = a+a+b+b+(-b) && \text{(Add } -b \text{ on the right)} \\
\overset{\cdot}{\iff} & a+b+a = a+a+b && \text{(Axiom i), associativity and inverse)} \\
\overset{\cdot}{\iff} & (-a)+a+b+a = (-a)+a+a+b && \text{(Add } -a \text{ on the right)} \\
\overset{\cdot}{\iff} & b+a = a+b && \text{(Axiom i), associativity and inverse)}
\end{aligned}$$