CKKS Lecture Notes

Part 0: Ring theory

FEI

October 2026

1 Review

1.1 Definitions and examples

Rings

A *commutative ring* is a set S with addition and multiplication operations that satisfy the following properties:

- **Identity.** There exist elements $0, 1 \in S$ such that for all $x \in S$, $0 + x = 1x = x$.
- **Commutativity.** For all $x, y \in S$, $x + y = y + x$ and $xy = yx$.
- **Associativity.** For all $x, y, z \in S$, $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$.
- **Distributivity.** For all $x, y, z \in S$, $x(y + z) = xy + xz$.
- **Additive inverse.** For all $x \in S$, there exists $-x \in S$ such that $x + (-x) = 0$.

We'll only use commutative rings here, so when we say "ring," we mean "commutative ring." A few examples of rings are:

- The integers $\mathbb{Z}$
- The real numbers $\mathbb{R}$
- The complex numbers $\mathbb{C}$

Product rings

Let $\mathcal{R}_1, \ldots, \mathcal{R}_n$ be rings. Then, the product ring $\mathcal{R}_1 \times \cdots \times \mathcal{R}_n$ is the set of n-tuples $(r_1, \ldots, r_n)$ with $r_i \in \mathcal{R}_i$.

For example, in $\mathbb{Z} \times \mathbb{C}$, we have

$$(2, 2.2i) \cdot (5, 3.5) + (1, 0.5) = (2 \cdot 5 + 1, 2.2i \cdot 3.5 + 0.5) = (11, 0.5 + 7.7i).$$

For a ring $\mathcal{R}$, we'll use $\mathcal{R}^n$ to denote the product ring of n copies of $\mathcal{R}$. In particular, $\mathbb{C}^n$ will refer to a ring, not a vector space.

Polynomial rings

Let $\mathcal{R}$ be a ring. Then, the set of single-variable polynomials with coefficients in $\mathcal{R}$ also forms a ring. We denote this $\mathcal{R}[X]$.

Quotient rings by a principal ideal

Let $\mathcal{R}$ be a ring. Let $r \in \mathcal{R}$. Define the equivalence relation $\sim_r$ on $\mathcal{R}$ such that $x \sim_r y$ if $x - y$ is a multiple of r.

The set of equivalence classes under $\sim_r$ also forms a ring, which we denote $\mathcal{R}/(r)$.

For instance, for $Q \in \mathbb{Z}$, $\mathbb{Z}/(Q)$ is the ring of integers modulo Q. From now on, we will denote this as $\mathbb{Z}_Q$.

We can also take quotient rings of polynomial rings. For example,

$$\mathbb{R}[X]/(X^4 + 1)$$

is the ring of real polynomials where X^4 is considered equal to -1.

1.2 Homomorphism

A homomorphism is a map between rings that preserves operations.

Homomorphism

Let $\mathcal{R}, \mathcal{S}$ be rings. A *homomorphism* is a function $f : \mathcal{R} \to \mathcal{S}$ such that:

- $f(1_{\mathcal{R}}) = 1_{\mathcal{S}}$ (i.e. the identity in $\mathcal{R}$ is mapped to the identity in $\mathcal{S}$).
- For all $x, y \in \mathcal{R}$, $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$.

Example: Polynomial evaluation

Given a polynomial ring $\mathcal{R}[X]$ and an element $a \in \mathcal{R}$, there is a homomorphism

$$\phi_a : \mathcal{R}[X] \to \mathcal{R}$$

that preserves elements of $\mathcal{R}$ and sends X to a.

In other words, ϕ_a sends a polynomial to its evaluation at a.

For example, in $\mathbb{R}[X]$,

$$\phi_3(X^2 + 2X + 5) = 3^2 + 2 \cdot 3 + 5 = 20.$$

Example: Polynomial evaluation in a quotient ring

Given a quotient ring $\mathcal{R}[X]/(f(X))$ and an element $a \in \mathcal{R}$ such that $f(a) = 0$, there is a homomorphism

$$\phi_a : \mathcal{R}[X]/(f(X)) \to \mathcal{R}$$

that preserves elements of $\mathcal{R}$ and sends X to a.

For example, because $i^2 + 1 = 0$, there is a homomorphism $\mathbb{C}[X]/(X^2 + 1) \to \mathbb{C}$ that preserves $\mathbb{C}$ and sends X to i.

However, there is no such homomorphism that sends X to 1. If there were such a homomorphism ϕ, we would have

$$0 = \phi(0) = \phi(X^2 + 1) = \phi(X)^2 + 1 = 2,$$

which is absurd.

In fact, this works for general $a \in \mathcal{R}[X]/(f(X))$, not just $a \in \mathcal{R}$.

More general statement

Given a quotient ring $\mathcal{R}[X]/(f(X))$ and an element $a \in \mathcal{R}[X]/(f(X))$ such that $f(a) = 0$, there is a homomorphism

$$\phi_a : \mathcal{R}[X]/(f(X)) \to \mathcal{R}[X]/(f(X))$$

that preserves elements of $\mathcal{R}$ and sends X to a.

1.3 Isomorphism

Isomorphism

An isomorphism is a homomorphism that is a bijection. We say $\mathcal{R}$ and $\mathcal{S}$ are isomorphic if there exists an isomorphism from $\mathcal{R}$ to $\mathcal{S}$.

Equivalently, an isomorphism is a homomorphism that has an inverse.

Automorphism

An automorphism is an isomorphism from a ring to itself.

For example, complex conjugation is an automorphism of $\mathbb{C}$.

2 Ring theory for CKKS

Let N be a power of 2. Let $k \in \mathbb{Z}$ be odd. Then,

$$(X^k)^N + 1 = (X^N)^k + 1 = (-1)^k + 1 = 0.$$

Fact

There is an automorphism

$$\sigma_k : \mathbb{R}[X]/(X^N + 1) \to \mathbb{R}[X]/(X^N + 1)$$

that fixes elements of $\mathbb{R}$ and sends X to X^k. A similar statement holds in $\mathbb{Z}_Q[X]/(X^N + 1)$.

Let $\zeta = e^{\frac{i\pi}{N}}$. Since $(\zeta^k)^N + 1 = 0$, there is a homomorphism

$$\phi_k : \mathbb{C}[X]/(X^N + 1) \to \mathbb{C}$$

that preserves elements of $\mathbb{C}$ and sends X to ζ^k. This homomorphism sends a polynomial f to its evaluation $f(\zeta^k)$.

Since $\mathbb{R}[X]/(X^N+1) \subseteq \mathbb{C}[X]/(X^N+1)$, ϕ_k also determines a homomorphism from $\mathbb{R}[X]/(X^N + 1)$ to $\mathbb{C}$.

Fact

There is a homomorphism

$$\phi_k : \mathbb{R}[X]/(X^N + 1) \to \mathbb{C}$$

that preserves elements of $\mathbb{R}$ and sends X to ζ^k.

Define

$$\Psi : \mathbb{C}[X]/(X^N + 1) \to \mathbb{C}^N$$

such that

$$\Psi(f) = (\phi_1(f), \phi_3(f), \cdots, \phi_{2N-1}(f)).$$

We claim Ψ is an isomorphism. Because each ϕ_k is a homomorphism, Ψ is a homomorphism.

A polynomial of degree less than N is uniquely determined by its evaluations at N points. So, Ψ is a bijection.

The powers of 5 cover all residues $r \pmod{2N}$ such that $r \equiv 1 \pmod 4$. Thus,

$$\zeta^1, \zeta^5, \ldots, \zeta^{5^{N/2-1}}$$

cover half of the primitive $2N$th roots of unity.

The other primitive $2N$th roots of unity are $\zeta^{-1}, \zeta^{-5}, \ldots, \zeta^{-5^{N/2-1}}$, which are the conjugates of these. A polynomial $f \in \mathbb{C}[X]/(X^N+1)$ has real coefficients if and only if

$$f(\zeta^{-5^k}) = f(\overline{\zeta^{5^k}}) = \overline{f(\zeta^{5^k})}$$

for each k. So, an element of $\mathbb{R}[X]/(X^N+1)$ is uniquely determined by its evaluations at

$$\zeta^1, \zeta^5, \ldots, \zeta^{5^{N/2-1}}.$$

Thus, we can define the isomorphism

$$\Phi : \mathbb{R}[X]/(X^N+1) \to \mathbb{C}^{N/2}$$

such that

$$\Phi(f) = (\phi_1(f), \phi_5(f), \phi_{5^2}(f), \cdots, \phi_{5^{N/2-1}}(f)).$$

Exercise

Define $\rho_k : \mathbb{C}^{N/2} \to \mathbb{C}^{N/2}$ such that

$$\rho_k((c_0, \ldots, c_{N/2-1})) = (c_k, \ldots, c_{N/2-1}, c_0, \ldots, c_{k-1}).$$

- Check that ρ_k is an automorphism.
- What automorphism of $\mathbb{R}[X]/(X^N+1)$ does this correspond to?

Define $\rho_{\text{conj}} : \mathbb{C}^{N/2} \to \mathbb{C}^{N/2}$ such that

$$\rho_{\text{conj}}((c_0, \ldots, c_{N/2-1})) = (\overline{c_0}, \ldots, \overline{c_{N/2-1}}).$$

- Check that ρ_{conj} is an automorphism.
- What automorphism of $\mathbb{R}[X]/(X^N+1)$ does this correspond to?

Solution

Let f be the element of $\mathbb{R}[X]/(X^N+1)$ that corresponds to $(c_0, \ldots, c_{N/2-1})$. In other words, $(c_0, \ldots, c_{N/2-1}) = \Phi(f)$. We have

$$\begin{aligned}
\rho_k((c_0, \ldots, c_{N/2-1})) &= \rho_k((\phi_1(f), \phi_5(f), \ldots, \phi_{5^{N/2-1}}(f))) \\
&= \rho_k((f(\zeta^1), f(\zeta^5), \ldots, f(\zeta^{5^{N/2-1}}))) \\
&= (f(\zeta^{5^k}), \ldots, f(\zeta^{5^{N/2-1}}), f(\zeta^1), \ldots, f(\zeta^{5^{k-1}})) \\
&= (\sigma_{5^k}(f)(\zeta^1), \ldots, \sigma_{5^k}(f)(\zeta^{5^{N/2-1}})).
\end{aligned}$$

So, $\Phi(\sigma_{5^k}(f)) = \rho_k(\Phi(f))$. So, applying ρ_k in $\mathbb{C}^{N/2}$ corresponds to

applying σ_{5^k} in $\mathbb{R}[X]/(X^N+1)$.

For similar reasons, applying ρ_{conj} in $\mathbb{C}^{N/2}$ corresponds to applying σ_{-1} in $\mathbb{R}[X]/(X^N+1)$.