FMCS:Math/April 9th, 2013

# Lecture 1

## 1 Review on Basic Algebra

### 1.1 Integer

- Prime $p$ ?
- Prime Factorization $n = p_1^{e_1} p_2^{e^2} \cdots p_m^{e_m}$ ?
- Division Theorem : $n = q \cdot m + r$ where $r < m$.
- Greatest Common Divisor $(n, m)$ ?
- Euclidean Algorithm ?
- Fermat's little theorem ?

### 1.2 Group

- Abelian Group $G$ ?
- (Normal) Subgroup $H \lhd G$ and Quotient Group $G/H$ ?
- Examples : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$.
- (Group) Homomorphism $f : G \to H$ and Isomorphism ?
- **Homomorphism Theorem :** If $f : G \to H$ is a surjective homomorphism, then $\bar{f} : G/\mathrm{Ker} f \to H$ is an isomorphism.
- **Fundamental Theorem of Abelian Groups :** A finitely generated abelian group is isomorphic to a product of cyclic groups in a unique manner.

### 1.3 Ring

- Commutative Ring with Unit $R$ ?
- Ideal $\mathfrak{a} \subset R$ ?
- Quotient Ring $R/\mathfrak{a}$ ?
- Examples : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/(n)$.
- (Ring) Homomorphism $f : R \to S$ and Isomorphism.

- **Homomorphism Theorem :** If $f : R \to S$ is a surjective homomorphism, then $\bar{f} : R/\mathrm{Ker} f \to S$ is an isomorphism.
- Integral Domain ?
- Principal Ideal Domain ?

## 1.4 Field

- Field $K$ ?
- Characteristic of Field ?
- (Field) Homomorphism $f : K \to L$ and Isomorphism ?
- Examples : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{F}_p$

## 1.5 Polynomial

- Polynomial Ring $K[X]$ ?
- **Division Theorem :** $f = q \cdot g + r$ where $\deg r < \deg g$.
- Greatest Common Divisor $(f, g)$.
- Euclidean Algorithm.
- **Theorem :** $K[X]$ is a principal ideal domai.
- Irreducible Polynomial over $K$.
- **Theorem :** If $f \in K[X]$ is irreducible, then $K[X]/(f)$ is a field.
- Examples : $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$, $\mathbb{Q}[X]/(X^2-2) \simeq \mathbb{Q}(\sqrt{2})$, $\mathbb{F}_2[X]/(X^2+X+1) \simeq \mathbb{F}_4$