Lecture 18 Groups, Rings, Fields and Ideals

1 Groups, Rings and Fields

Definition 1. *A group consists of a set G and a binary operation "$\cdot$" defined on G, for which the following conditions are satisfied:*

1. *Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.*
2. *Identity: There exists an element $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$.*
3. *Inverse: Given $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = 1$.*

Examples: $\mathbb{S}_n$ of permutations on $[n]$, $GL(n, \mathbb{R})$ of real nonsingular $n \times n$ matrices under matrix multiplication.

If we drop the condition on the existence of an inverse, we obtain a **monoid**. Note that a monoid always has at least one element, the identity. As an example, given a set S, then the set of all strings of elements of S is a monoid, where the monoid operation is string concatenation and the identity is the empty string λ. Monoids are also known as semigroups with identity.

Definition 2. *A ring consists of a set R and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:*

1. *Additive associative: $(a + b) + c = a + (b + c)$, for all $a, b, c \in R$.*
2. *Additive commutative: $a + b = b + a$, for all $a, b \in R$.*
3. *Additive identity: There exists an element $0 \in R$ such that for all $a \in R$, $0 + a = a + 0 = a$.*
4. *Additive inverse: for every $a \in R$, there exists $-a \in R$ such that $a + (-a) = (-a) + a = 0$.*
5. *Left and right distributivity: For all $a, b, c \in R$, it holds that $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.*
6. *Multiplicative associativity: For all $a, b, c \in R$, it holds that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

If R is multiplicatively commutative, then it is a commutative ring.
Examples: $\mathbb{Z}$ under the usual addition and multiplication, $\mathbb{R}[x], \mathbb{C}[x]$.

Definition 3. *A field consists of a set F and two binary operations "$+$" (addition) and "$\cdot$" (multiplication), defined on R, for which the following conditions are satisfied:*

1. *$(F, +, \cdot)$ is a ring.*
2. *Multiplicative commutative: For any $a, b \in F$, $a \cdot b = b \cdot a$.*

3. *Multiplicative identity: There exists* $1 \in F$ *such that* $a \cdot 1 = 1 \cdot a = a$ *for all* $a \in F$.

4. *Multiplicative inverse: If* $a \in F$ *and* $a \neq 0$, *there exists* $b \in F$ *such that* $a \cdot b = b \cdot a = 1$.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Q}(x), \mathbb{R}(x), \mathbb{C}(x)$.

A field k is algebraically closed if every nonzero polynomial $p(x) \in k[x_1, \ldots, x_n]$ has at least a root in k.

2 Ideals

Definition 4. *Let* R *be a commutative ring. A subset* I *of* R *is an ideal if*

- *If* $a, b \in I$, *then* $a + b \in I$.
- *If* $a \in I$ *and* $b \in R$, *then* $ab \in I$.

Theorem 5 (Hilbert's Basis Theorem)**.** *Let* k *be a field, and* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. Then there exist polynomials* $g_1, \ldots, g_s$ *such that*

$$I = \langle g_1, \ldots, g_s \rangle.$$

That is, for every $f \in I$, *there exist polynomials* $f_1, \ldots, f_s$ *such that*

$$f = f_1 g_1 + \cdots + f_s g_s.$$

Such g_i *is called a generator of* I.

Definition 6. *Let* k *be a field, and* $f_1, \ldots, f_m$ *be polynomials in* $k[x_1, \ldots, x_n]$. *Let the set* V *be*

$$V(f_1, \ldots, f_m) = \{(u_1, \ldots, u_n) \in k^n : \ f_i(u_1, \ldots, u_n) = 0, \, i = 1, \ldots, m\}.$$

The set $V(f_1, \ldots, f_m)$ *is called the affine variety defined by* $f_1, \ldots, f_m$.

Let V be a variety. The set

$$I(V) = \{f \in k[x_1, \ldots, x_n] : \ f(u_1, \ldots, u_n) = 0, \quad \forall \, u \in V\}$$

is an ideal of the ring $k[x_1, \ldots, x_n]$. It is called the vanishing ideal of V.

Definition 7. *Let* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. The radical ideal of* I, *denoted by* $\sqrt{I}$, *is the set*

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] : \ \exists p \in \mathbb{N}, \ f^p\}.$$

If $I = \sqrt{I}$, *we say* I *is a radical ideal.*

For example $I =< x^m, y^n >$ is not radical, and $\sqrt{I} =< x, y >$. For every V, the vanishing ideal $I(V)$ is radical.

Theorem 8 (Hilbert's Nullstellensatz)**.** *Let* k *be an algebraically closed field, and* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. Then* $I(V(I)) = \sqrt{I}$.