Lecture 1: January 17

Lecturer: Himanshu Shukla *Scribe: Siddharth Agrawal*

1.1 Ideals

From henceforth R will denote a commutative ring with the multiplicative identity.

Definition 1.1 *A set $I \subseteq R$ is an ideal of R if:*

- *I is a subgroup of R under addition.*
- *$\forall r \in R$, $r \bullet I \subseteq I$*

Here is a list of few basic definitions from ring theory

- An ideal is said to be *proper* if $I \subsetneq R$.
- A proper ideal I is said to be a **Maximal** if for an ideal J of R, $I \subsetneq J$ then $J = R$.
- An ideal P is said to be *prime* if
$$\alpha \bullet \beta \in P \Rightarrow \alpha \in P \mid \beta \in P$$

Lemma. $R \backslash I$ is a field or an integral domain *iff* I is a maximal ideal or I is a prime ideal respectively.

1.2 Module

A *module* can be thought of as a vector space over a ring (instead of a field).
Definition. A module M over a ring R is such that $\exists \varphi : R \times M \to M$ satisfying:

- $r_1(r_2 \bullet m) = (r_1 r_2) \bullet m$
- $(r_1 + r_2) \bullet m = r_1 \bullet m + r_2 \bullet m$
- $r \bullet (m_1 + m_2) = r \bullet m_1 + r \bullet m_2$

Example: Every ideal is a module over its underlying ring.

1.3 Extensions of Fields

If a field $F \subset E$, then E is said to be an *extension* of F. It is trivial to see that E forms a vector space over the field F. Depending on the finiteness of the basis of this vector space, we have *finite* or *infinite* extensions.
$(\overline{\mathbb{Q}} : \mathbb{Q}) := \overline{\mathbb{Q}}$ is an extension of $\mathbb{Q}$.
$[E : F] :=$ dimension of the vector space E over the field F.

Note. Integral Domain $\supset$ Unique Factorisation Domain $\supset$ Principle Ideal Domain $\supset$ Euclidean Domain $\supset$ Field

Definition. R is a *Euclidean domain* if $\exists$ a map $\varphi : R \to Z_+$ such that $\forall a, b \in R, b \neq 0, \exists q, r$ such that

$$a = bq + r,\ \varphi(b) > \varphi(r)\ or\ r = 0$$

Example: $F[x]$ is a Euclidean domain.

Definition. R is a principle ideal domain (PID) if $\forall p, q \in R$, $\exists x, y$ s.t.,

$$px + qy = gcd(p, q)$$

Note: If R is a PID, but not a Euclidean domain, then we dont have a algorithm to find these x and y values, although it is proven that they must exist.

Let $\alpha \in\ E\ \supseteq\ F$, then α is called *algebraic* over F if
$\exists (a_0, a_1, ..., a_n) \in \mathbb{F}_{n+1}$ s.t.,

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0$$

i.e. $\exists\ p(x) \in F[x]$ s.t. $p(\alpha) = 0$.
An extension E of a field F is said to be algebraic if every element of E is algebraic over F.

Let $\varphi\ : F[X] \to E$, $X \mapsto \alpha$
Observation. α is algebraic *iff* φ has a non-trivial kernel.

Now, by the second isomorphism theorem,

$$\frac{F[X]}{ker(\varphi)} \cong F[\alpha]$$

. Since $F[X]$ is a Euclidean domain. therefore F[X] is definitely a PID. Also, $ker(\varphi)$ is an ideal under all circumstances. Therefore, $ker(\varphi)$ has to be a principle ideal of $F[X]$,

$$\Rightarrow \exists\ p(X) \in F[X]\ s.t.\ ker(\varphi) = (p(X))$$

Claim. $p(X)$ is unique and irreducible, & $p(\alpha) = 0$.
(Proof left as an Exercise)

Proposition. If E is finite over F, then E is algebraic over F.
Proof: $\forall \alpha \in E, \exists n$ s.t. $1, \alpha, ..., \alpha^n$ is linearly dependant.

Theorem. Let $K \subseteq F \subseteq E$ be fields, then

$$[F : K][E : F] = [E : K]$$

Note: We have not assumed anything regarding the finiteness of F and E as extensions, i.e. this theorem is valid even for infinite bases.
If $(\alpha_i),\ i \in I$ is an infinite basis of a vector space E over a fiels F, then

$$\forall \beta \in E,\ \beta = \sum_{i \in I} c_i \alpha_i,\ where\ only\ finitely\ many\ c_i \neq 0$$

Let $K(\alpha)$ be the smallest field containing α nad K, i.e. it is the smallest extension of the field K that contains α.

Proposition. (i) $K[\alpha] = K(\alpha)$ (ii) $[K(\alpha) : K] = deg(Irr(\alpha, K, X))$