MATH 8510 GALOIS THEORY

LU JUNYU

1. Week 1

Let's agree on some facts and conventions from elementary abstract algebra, in particular those with polynomial rings before we dig into Galois theory.

A ring is always commutative with multiplicative identity 1 unless otherwise stated. R^* is the multiplicative group of units in R and $R^\times = R \setminus \{0\}$. We can use these two notations interchangeably when R is a field.

Let F be a field. A polynomial ring $F[X]$ with an indeterminate X is an F-vector space with basis $1, X, X^2, ..., X^n, ...$ with the multiplication

$$(\sum_i a_i X^i)(\sum_j b_j X^j) = \sum_k (\sum_{i+j=k} a_i b_j) X_k,$$

where X^0 is defined to be 1. Alternatively, we can identify $R[X]$ with

$$R^{(\mathbb{N})} = \{(a_i) : a_i \in R, a_i = 0 \text{ for all but finitely many } i \in \mathbb{N}\}$$

in an obvious way. The degree function has the following properties:

(1) $\deg(f+g) \leq \max(\deg f, \deg g)$,
(2) $\deg(fg) = \deg f + \deg g$.

Theorem 1.1. *Let F be a commutative ring. Then $F[X]$ is a PID if and only if F is a field.*

Hence or otherwise $\mathbb{Z}[X]$ is not a PID. Indeed, $\langle 2, X\rangle$ is an example of an ideal that cannot be generated by a single polynomial. $K[X,Y]$ is not a PID as $\langle X, Y\rangle$ is not principal.

Theorem 1.2. *An ideal in a PID is prime if and only if it is maximal.*

Theorem 1.3 (Gauss's Lemma)**.** *A polynomial $f(X) \in \mathbb{Z}[X]$ is irreducible if and only if it is irreducible over $\mathbb{Q}[X]$.*

Theorem 1.4 (Eisenstein Criterion)**.** *Let $f(X) = a_0 + a_1 X + ... + a_n X^n \in \mathbb{Z}[X]$ be a polynomial over integers with $a_n \neq 0$. Suppose that there exists a prime p such that*

(1) $p \nmid a_n$,
(2) $p \mid a_i$ *for* $i = 0, 1, ..., n-1$,
(3) $p^2 \nmid a_0$.

Then $f(X)$ is irreducible over $\mathbb{Z}[X]$.