MATH 8510 Galois Theory

LU Junyu

January 15, 2021

Week 1

0.1 Warm up

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. But usually, we want to say R embeds into $R[X]$ although the most formal way is to identify R with a subring of $R[X]$. The degree function has the following properties:

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

There are plenty results by arguing over the degree of a polynomial. We have $(R[X])^* = R^*$ if R is an integral domain. We have the division algorithm on $R[X]$.

Theorem 0.1. *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 0.2. *An ideal in a PID is prime if and only if it is maximal.*

Definition 0.3. If $f(X) \in F[X]$ where F is a field, then a **root** of f in F is an element $\alpha \in F$ such that $f(\alpha) = 0$.

Given a polynomial $f[X] \in F[X]$ and any $u \in F$, the division algorithm give us:

$$f(X) = q(X)(X - u) + f(u).$$

And lying in the center of proving that every finite subgroup of $F^{\times}$ is cyclic is counting the roots of polynomial $X^n - 1$.

Theorem 0.4. *Let F be a field and $f[X] \in F[X]$ a polynomial of degree n. Then f has at most n roots.*

Definition 0.5. Let F be a field. A nonzero polynomial $p(X) \in F[X]$ is said to be **irreducible** over F (or **irreducible** in $F[X]$) if $\deg p \geq 1$ and there is no factorization $p = fg$ in $F[X]$ with $\deg f < \deg p$ and $\deg g < \deg p$.

A quadratic or cubic polynomial is irreducible in $F[X]$ if and only if it has no root in F.

Theorem 0.6 (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 0.7 (Eisenstein's 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 $\mathbb{Z}[X]$.

A typical application of Eisenstein's Criterion is to prove the irreducibility of the p-th cyclotomic polynomial $\Phi_p(X) = \frac{X^p - 1}{X - 1}$, where p is a prime. The idea is to apply the criterion to $\Phi(X + 1)$.

Theorem 0.8. *Let F be a field and $f(x)$ a polynomial in $F[X]$. Then $(f(X))$ is a prime ideal in $F[X]$ if and only if $f(X)$ is irreducible. Equivalently, f is irreducible if and only if $K[X]/(f)$ is a field.*

Making use of above results, we finally reach the very last theorem which functions as a cornerstone in many arguments.

Theorem 0.9. *Let k be a field and $f[X]$ a monic irreducible polynomial in $k[X]$ of degree d. Let $K = k[X]/I$, where $I = (f)$, and $\beta = X + I \in K$. Then:*

1. *K is a field and $k' = \{a + I : a \in k\}$ is a subfield of K isomorphic to k,*
2. *β is a root of g in K,*
3. *if $g(X) \in k[X]$ and β is a root of g in K, then $f \mid g$ in $k[X]$,*
4. *f is the unique monic irreducible polynomial in $k[X]$ having β as a root,*
5. *$1, \beta, \beta^2, ..., \beta^{d-1}$ forms a basis of K as a vector space over k and so $\dim_k(K) = d$.*

0.2 Extensions of fields

Most of this course will involve studying fields relative to certain subfield which we feel we understand better. For example, if $\alpha \in \mathbb{C}$ is the root of some polynomial with coefficients in $\mathbb{Q}$, we might wish to study $\mathbb{Q}(\alpha)$, the smallest subfield of $\mathbb{C}$ containing α and all of $\mathbb{Q}$. Certainly, if we want to understand how "complicated" the number α is, it makes sense to consider how "complicated" the field $\mathbb{Q}(\alpha)$ is as an extension of $\mathbb{Q}$. If $F \subset E$ are fields, we will denote denote the extension by E/F (this just means that F is a subfield of E, and that we're considering E relative to F, in particular, E/F is not a quotient or anything too formal). Note that often we will consider E to be an extension of F even if $F \nsubseteq E$, as long as there is an obvious embedding of F into E (an embedding is a homomorphism with is injective).

We will make a lot of use of the observation that if E/F is an extension of fields, then we may view E as a vector space over F.