MATH 8510 Galois Theory

LU Junyu

Week 1

1.1 Review on polynomial rings

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 $1, X, X^2, \cdots, X^n, \cdots$, 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

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

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 $R[X]$. We will also use notations like $F[x], k[x]$ and $k[X]$ for polynomial rings as long as there is no confusion.

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 1.1.1. *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 1.1.2. *An ideal in a PID is prime if and only if it is maximal.*

Definition 1.1.3. 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 1.1.4. *Let F be a field and $f[X] \in F[X]$ a polynomial of degree n. Then f has at most n roots.*

Definition 1.1.5. 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 1.1.6 (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 1.1.7 (Eisenstein's Criterion)**.** *Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ 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 $i = 0, 1, \cdots, n-1$,*
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 1.1.8. *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.*

1.2 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.

Definition 1.2.1. Let E/F be an extension of fields. We say that E is a *finite extension* of F if E is finite-dimensional as a vector space over F. In this case we denote the dimension by $[E : F]$. We say that E is an *infinite extension* of F if E is infinite-dimensional as a vector space over F, and we write $[E : F] = 1$.

Example 1.2.2. $\{1, i\}$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$. So $\mathbb{C}$ is a finite extension of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.

Example 1.2.3. It is widely known that $\sqrt{2} \notin \mathbb{Q}$. Thus $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$. On the other hand $(\sqrt{2})^2 \in \mathbb{Q}$ and then any polynomial in $\sqrt{2}$ with rational coefficients is just a $\mathbb{Q}$-linear combinations of 1 and $\sqrt{2}$. Since

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$

every rational function of $\sqrt{2}$ can be written as a $\mathbb{Q}$-linear combinations of 1 and $\sqrt{2}$. It follows immediately that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ and $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Example 1.2.4. We can show $[\mathbb{C}(x) : \mathbb{C}] = \infty$ by arguing $\{1, x, x^2, \cdots\}$ is a linear independent set.

Example 1.2.5. To show $[\mathbb{R} : \mathbb{Q}] = \infty$, we make use of the unique factorization theorem of integers and argue that $\{\ln(p) : p \text{ is a prime}\}$ is a linearly independent set.

Theorem 1.2.6. *Let $K \subseteq F \subseteq E$ be fields. Then E/K is a finite extensions if and only if both F/K and E/F are, and when this is the case, we have*

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

Sketch of proof. If $\{a_i\}$ and $\{b_j\}$ are bases for E/F and F/K respectively, then $\{a_i b_j\}$ is a basis for E/K. □

Example 1.2.7. Consider field extensions $\mathbb{Q} \subset E = \mathbb{Q}[\sqrt{2}] \subset F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. We already know $[E : \mathbb{Q}] = 2$ and since $\sqrt{3} \notin E$ and it is a $x^2 - 3 \in E[x]$, we also have $[F : E] = [E[\sqrt{3} : E] = 2$. And then $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$.

Definition 1.2.8. Let E/F be a field extension. An element $\alpha \in E$ is *algebraic* over F if there is a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise we say that α is *transcendental* over F. The extension E/F is *algebraic* if every element of E is algebraic over F, and is *transcendental* otherwise.

Example 1.2.9. Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ as they are roots of $x^2 - 2$ and $x^2 + 1$. But π and e are transcendental. As you can see, it's much easier to show that something is algebraic over a subfield than to show that it isn't (since to show that it is, one simply needs to exhibit a non-trivial polynomial relation). This shows that $\mathbb{R}/\mathbb{Q}$ is a transcendental extension, but some more work is required to show that $\mathbb{Q}(\sqrt{2})$ is algebraic, namely, we need to make sure that the smallest field containing $\mathbb{Q}$ and $\sqrt{2}$ doesn't somehow contain transcendental elements over $\mathbb{Q}$.

Theorem 1.2.10. *Let E/F be a finite extension of fields. Then every element of E is algebraic over F. Specifically, for every element $\alpha \in E$ there is a unique non-zero monic irreducible polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$, and $f(x)$ divides every polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$. And this polynomial satisfies $deg(f) \leq [E : F]$. Moreover, if $I = (f)$, then $F[x]/I \cong k(\alpha)$; indeed, there exists an isomorphism $\phi : F[x]/I \to k(\alpha)$ with $\phi(x + I) = \alpha$ and $\phi(a + I) = a$ for all $a \in F$.*

Proof. Suppose that E/F is a finite extension and $\alpha \in E$. Consider the elements

$$1, \alpha, \alpha^2, \cdots, \alpha^{[E:F]} \in E.$$

Since there are $[E : F] + 1$ elements, they must be linearly dependent over F. Hence we can find $c_i \in F$ such that

$$c_o \cdot 1 + c_1\alpha + \cdots + c_{[E:F]}\alpha^{[E:F]} = 0.$$

In other words, α is a root of the (non-zero) polynomial

$$g(x) = \sum_{i=0}^{[E:F]} c_i x^i \in F[x].$$

And the degree of g is at most $[E : F]$.

Now consider the evaluation map

$$\varphi : F[x] \to E, f(x) \mapsto f(\alpha),$$

where one may consider it as the restriction of $e_\alpha : E[x] \to E$. Then $\ker(\varphi)$ is non-empty since g lies in it and then $\ker(\varphi) = (f(x))$ for some monic $f(x) \in F[x]$ since $F[x]$ is a PID. Any polynomial $g(x) \in F[x]$ with a root α belongs to the kernal and hense is divisible by $f(x)$. Clearly, $\deg f$ is no bigger than $\deg g$ and then no bigger than $[E : F]$. Since E is a field as well, im(φ) is a domain. So the kernel is a prime (hence maximal) ideal and therefore f is irreducible and im(φ) is a field containing $\mathbb{Q}$ and α indeed. ϕ is the canonical isomorphism induced by φ. □

Hence, we have $F[\alpha] = F(\alpha)$ when α is algebraic.

Definition 1.2.11. The polynomial f constructed in Theorem 1.2.10 is called the *minimal polynomial* of α over F.

In other words, in a finite extension, every element is the root of some polynomial over the smaller field. The next theorem is a partial converse to this, and we will use it often.

Theorem 1.2.12. *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 f 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. *$1, \beta, \beta^2, \cdots, \beta^{d-1}$ form a basis of K as a vector space over k and so $\dim_k(K) = d$.*

Proof. With the knowledge form the warm-up part, we can prove this theorem easily.

1. I is a prime ideal hence maximal since $F[x]$ is a PID. So the quotient ring $K = k[x]/I$ is a field. Every field homomorphism is injective and so k embeds into K with its image k'.

2. Let $f(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$, where $a_i \in k$ for all i. In $K = k[x]/I$, we have

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1 x + I) + \cdots + (x^d + I) \\ &= a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d + I \\ &= f(x) + I = 0 + I. \end{aligned}$$

   So β is a root of p.

3. If $f \nmid g$ in $k[x]$, then their $\gcd$ is 1 since f is irreducible. Therefore, we can find polynomials s, t in $k[x]$ such that $1 = sf + gt$. Treating them as polynomials in $K[x]$ and evaluating at β, we get $1 = 0$, a contradiction.

4. Let g be a monic irreducible polynomial in $k[x]$having β as a root. Then by part (3) we have $f \mid g$. Since g is irreducible, we have $g = ch$ for some constant c. But both f, g are monic, we have $c = 1$ and $f = g$.

5. Every element of K has the form $g + I$, where $g(x) \in k[x]$. By the division algorithm, we have $g = qf + r$ with either $r = 0$ or $\deg(r) < \deg(f)$. Then $g + I = r + I$ since $g - r = qf \in I$. By the calculation similar in part (2), it follows that $r + I = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$ if we express $r(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$.

   If $\{1, \beta, \beta^2, \cdots, \beta^{d-1}\}$ is not linearly independent, then we can find coefficients $c_i \in k$ not all zero such that
$$c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1} = 0.$$
   Define $g(x) \in k[x]$ by $f(x) = \sum_{i=0}^{d-1} c_i x^i$. Then $g(\beta) = 0$ and $\deg(g) \leq d-1 < \deg(f) = d$. By part (3) says $\deg(f) \leq \deg(g)$ since $f \mid g$. We reach a contradiction.

□

Remark. The pair (K, β) is called the *stem field* in Milner.

Example 1.2.13. The polynomial $x^2 + 1 \in \mathbb{R}[x]$ is irreducible so $K = \mathbb{R}[x]/(x^2 + 1)$ is a finite extension of $\mathbb{R}$ with degree 2. If β is a root of $x^2 + 1$ in K, then $\beta^2 = -1$. Moreover, every element of K has a unique expression $a + b\beta$, where $a, b \in \mathbb{R}$.

Example 1.2.14. Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[X]$. This is an irreducible polynomial: it has no rational roots (if r/s in lowest form was one, then $r \mid 1$ and $r \mid 1$; the only possible rational root was $r/s = \pm 1/1 = \pm 1$) and a direct factorization $f(x) = (x^2 + ax + b)(x^2 - ax + c)$ is also impossible. (One can show, however, f is reducible in $\mathbb{F}_p[x]$ for any prime p.) The roots of f are

$$\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}.$$

Let β be one of the roots. Consider the field extensions $\mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. We already know from pervious example

$$[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4 = [\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\beta]][\mathbb{Q}[\beta] : \mathbb{Q}].$$

But β is a root of irreducible polynomial of degree 4 and therefore

$$[\mathbb{Q}[\beta] : \mathbb{Q}] = 4.$$

We see that $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\beta]] = 1$ and then

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\beta].$$

And hence all roots of f lies in $\mathbb{Q}[\beta]$.

1.3 Automorphisms

When one is first introduced to the complex numbers, it is usually as a superset of the reals. We're introduced to $\mathbb{C}$ as a vector space over $\mathbb{R}$ with basis $\{1, i\}$ which happens to also admit the structure of a field. One function which helps with the very basic study of $\mathbb{C}$ from this perspective is the complex conjugation:

$$\overline{x + yi} = x - yi$$

for $x, y \in \mathbb{R}$. The important properties of this function are that it is an automorphism of $\mathbb{C}$ and that it fixes real numbers (and only real numbers. We would like to identify functions of this form for arbitrary field extensions.

Definition 1.3.1. Let F be a field, and let $X \subset F$ be a subset. Then $\varphi : F \to F$ is an automorphism if it is a bijection and a homomorphism, namely, $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$. We denote the group of automorphisms of F by $\mathrm{Aut}(F)$. We say that $\varphi \in \mathrm{Aut}(F)$ fixes X if $\varphi(x) = x$ for all $x \in X$, and we denote the set of automorphisms of F fixing X by $\mathrm{Aut}(F/X)$.

It's worth noting that this definition of fixing a set is what might more rightly be referred to as fixing X pointwise. It is sometimes useful to consider functions which fix X setwise, meaning that $\varphi(x) \in X$ for all $x \in X$. Unless otherwise stated, "fix" means "fix pointwise". Note that, in the lemma below, we make no special assumptions about the nature of $X \subset F$.

Proposition 1.3.2. *For any field F, and any set $X \subset F$, the set $\mathrm{Aut}(F/X)$ is a group under composition.*

Proof. Just straightforward verifications. □

Example 1.3.3. Consider Aut($\mathbb{C}/\mathbb{R}$). Every element of $\mathbb{C}$ can be written as $x + yi$ with $x, y \in \mathbb{R}$. For any $\sigma \in$ Aut($\mathbb{C}/\mathbb{R}$), we must have $\sigma(x + yi) = x + y\sigma(i)$. Furthermore, we also have

$$-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2,$$

and hence $\sigma(i) = \pm i$. So Aut($\mathbb{C}/\mathbb{R}$) contains exactly two elements: the trivial one and the complex conjugation. It is clear that Aut($\mathbb{C}/\mathbb{R}$) is group — we need to check the complex conjugation is an automorphism of $\mathbb{C}$ and twice the complex conjugation is just the identity map.

This example gives us a feeling about how Aut(E/F) will be for a field extension E/F. In general, if E/F is a finite extension with $[E : F] = n$, then we can choose a basis $\alpha_1, \cdots, \alpha_n \in E$ for E/F. Any element of E can be written uniquely in the form

$$c_1\alpha_1 + \cdots + c_n\alpha_n,$$

with $c_i \in F$. If $\sigma \in$ Aut(E/F), then we have

$$\sigma(c_1\alpha_1 + \cdots + c_n\alpha_n) = c_1\sigma(\alpha_1) + \cdots + c_n\sigma(\alpha_n).$$

In other words, the automorphism σ is entirely defined by the n values $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$. Moreover, if $f_i(x) \in F[x]$ is the minimal polynomial for α_i, then

$$f_i(\sigma(\alpha_i)) = \sigma(f_i(\alpha_i)) = \sigma(0) = 0.$$

So $\sigma(\alpha_i)$ is one of the (finitely many) roots of f_i in E. So there are only finitely many possible values for $\sigma(\alpha_i)$, for each i. We won't count how many automorphisms the can be (this will become easier later), but we've just made the following useful observation:

Theorem 1.3.4. *Let E/F be a finite extension of fields. Then Aut(E/F) is a finite group. Moreover, if we have $E = F(\alpha)$ for some $\alpha \in E$, then Aut(E/F) naturally embeds into the group of permutations of the roots of the minimal polynomial of α over F.*

Note that E/F does not need to be a finite extension for us to define Aut(E/F) (indeed, F need not even be a field). Unfortunately, there are interesting extensions E/F for which the group Aut(E/F) is not interesting.

Example 1.3.5. Let α be the real cube root of 2, and let $E = \mathbb{Q}(\alpha)$. Then $[E : \mathbb{Q}] = 3$ (since the minimal polynomial of α, which is $f(x) = x^3 - 2$, is irreducible over $\mathbb{Q}$). Now suppose that $\sigma \in$ Aut(E/Q). We've seen that σ is entirely determined by $\sigma(\alpha)$. But $E \subset \mathbb{R}$, and $\sigma(\alpha)$ has to satisfy

$$\sigma(\alpha)^3 = \sigma(\alpha^3) = 2.$$

In particular, $\sigma(\alpha)$ is a real cube root of 2, and so the only possibility is $\sigma(\alpha) = \alpha$. In other words, the only element of Aut(E/Q) is the trivial element $\sigma(x) = x$ for all $x \in E$.

This example is somewhat unsatisfying. One of the important properties of the group Aut($\mathbb{C}/\mathbb{R}$) is that the non-trivial element fixes exactly $\mathbb{R}$. In the example above, the (trivial) group Aut($E/\mathbb{Q}$) isn't going to be of much use in studying the field E. In some sense, the problem is that E contains only one cube root of 2, but we expect there to be 3 distinct cube roots of 2; we'll explore this more when we define what it means for an extension to be Galois.

Example 1.3.6. We can show Aut($\mathbb{R}/\mathbb{Q}$) is also trivial. Let $\sigma \in$ Aut($\mathbb{R}/\mathbb{Q}$). From the observation that

$$\sigma(a^2) = \sigma(a)^2 > 0,$$

we see σ must take positive to positive and hence order-preserving. And then it must be continuous (by more detailed arguments) but any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map (again you may fill the details if you want).

Our next example says something about finite fields. We do a quick catch-up here.

We denote the finite field of order p, where p is a prime, by $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$. If F be a finite field with q elements and suppose that $F \subset K$ where K is also a finite field. Then K has q^n elements where $n = [K : F]$ from the knowledge on finite field extensions. Hence a finite field is isomorphic to $\mathbb{F}_{p^n}$ where p is its characteristic and $n \in \mathbb{N}$ — we will show any two fields have the same number of elements are isomorphic.

Since $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, we have $a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}$. The polynomial $x^{p^n} - x$ has at most $\deg = p^n$ roots and we conclude

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a) \in \mathbb{F}_{p^n}[x].$$

As we will see later, $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x \in \mathbb{F}[x]$.

Example 1.3.7. Let p be a prime, and consider the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. We define a function $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by $\sigma(x) = x^p$. By the binomial theorem, and the fact that p divides the binomial coefficient $\binom{p}{j}$for any $1 \le j \le p-1$, we have

$$\sigma(x + y) = (x + y)^p = x^p + y^p + p \cdot \text{(something)} = \sigma(x) + \sigma(y).$$

And of course $\sigma(xy) = \sigma(x)\sigma(y)$. So σ is a homomorphism. We wish to show that σ is an automorphism of $\mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n}$ is finite, we simply need to show that σ is either surjective or injective. We'll show that it's injective. To see this, suppose to the contrary that there's some non-zero $x \in \mathbb{F}_{p^n}$ with $\sigma(x) = 0$. Since the group of non-zero elements $\mathbb{F}_{p^n}$ is cyclic, say, generated by γ. If $x = \gamma^j$, then

$$x^{p^n} = (\gamma^j)^{p^n} = (\gamma^{p^n})^j = \gamma^j = x.$$

On the other hand,

$$x^{p^n} = \sigma^{(n)}(x) = \sigma^{n-1}(\sigma(x)) = \sigma^{(n-1)}(0) = 0,$$

where $\sigma^{(n)}$ means compose σ with itself n times. We reach a contradiction. Also, note that σ fixes $\mathbb{F}_p$, so really $\sigma \in$ Aut($\mathbb{F}_{p^n}/\mathbb{F}_p$). It's possible to show that σ generates this group (laster).

Week 2

2.4 Separable extensions

Let $f(x) \in F[x]$ be an irreducible polynomial and $(E = F[\alpha], \alpha)$ its stem field (or E a field containing all the roots). From what we have learnt from last week, we know an element in Aut(E/F) shall permute the roots of f. It then follows not surprisingly that we want the distinctness of the roots; in other words, we want the roots are separable.

Definition 2.4.1. Let k be a field. A nonzero polynomial $f(x) \in k[x]$ is called *separable* if it has no repeated roots (in any extension field).

Recall that the derivative of a polynomial $f(x) = \sum a_i x^i$ is defined to be $f'(x) = \sum i a_i x^{i-1}$. When f has coefficients in $\mathbb{R}$, this agrees with the definition in calculus. The usual rules for differentiating sums and products still hold, but note that in characteristic p the derivative of x^p is zero.

Theorem 2.4.2. *Let K be a field. An irreducible f polynomial in $K[X]$ is separable if and only if* $\gcd(f, f') = 1$ *in* $K[X]$.

Proof. Let $f(X)$ be an irreducible polynomial in $K[X]$. Suppose $f(X)$ is separable, and let α be a root of $f(X)$ (in some extension of K. Then $f(X) = (X - \alpha)h(X)$ for some $h(x) \neq 0$. Since $f'(\alpha) = h(\alpha) \neq 0$, f' is non-zero and $\deg(f') < \deg(f)$. It follows from the irreducibility of f immediately that $\gcd(f, f') = 1$.

Now suppose $f(X)$ is not separable and α is a repeated root (in an extension field). Then we can write $f(X) = (X - \alpha)^2 g(X)$ (in some extension field), where $g(x)$ is non-zero, and then $f'(X) = (X - \alpha)^2 g'(X) + 2(X - \alpha)g(x)$. It follows that f' is non-zero as well and $f'(\alpha) = 0$. By Theorem 1.2.10, both f, f' are divisible by the minimal polynomial of α in $K[X]$ and then $\gcd(f, f') \neq 1$. $\square$

Definition 2.4.3. A field F is said to be *perfect* if every irreducible polynomial in $F[x]$ is separable.

Fortunately, almost all the fields we have good feelings at are perfect.

Theorem 2.4.4. *A field F is perfect if and only if either F has characteristic* 0*, or F has characteristic p and the function $\sigma(x) : F \to F, x \mapsto X$ is an isomorphism. (And then in particular, any finite field is perfect.)*

Proof. Suppose that F has characteristic 0. Let f be an irreducible polynomial. Then $\deg(f') = \deg(f) - 1 \neq 0$ and it follows from the irreducibility of f that $\gcd(f, f') = 1$. Therefore, f is separable by Theorem 2.4.2.

Now consider the case when the characteristic of F is a prime p. We already see σ is a field homomorphism last week. Since field homomorphisms are injective, we only need to consider the surjectivity of σ.

Suppose that σ is not surjective and $a \in F$ is not in the image. Then the polynomial $f(x) = x^p - a$ has no roots in F.

Claim: $f(x)$ is irreducible.

Proof of claim: By Theorem 1.2.12, let E/F be a finite extension containing a root β of f and so that

$$f(x) = x^p - a = x^p - \beta^p = (x - \beta)^p \in E[x].$$

Thus if f factors non-trivially in $F[x]$, then a factor of f looks like $(x - \beta)^j \in F[x]$ for some $1 \le j < p$. The coefficient of x^{j-1} in $(x - \beta)^j$ is $-j\beta$. Since $j \neq 0$ in F, we conclude β lies in F and reach a contradiction.

Notice that $f'(x) = px^{p-1} = 0$ in $F[x]$. So every root of f is a multiple root. We have shown f is irreducible and inseparable and then F is not perfect.

For another direction, suppose that σ is surjective and that $f \in F[x]$ is irreducible and inseparable. Similarly to the argument in Theorem 2.4.2, we get f divides f'. If f' was not the zero polynomial, then $\deg(f') < \deg(f)$, which is impossible given $f \mid f'$. Let $f(x) = \sum_{i=0}^{d} a_i x^i$ then we get

$$0 = f'(x) = \sum_{i=1}^{d} i a_i x^{i-1} \in F[x].$$

Therefore, $ia_i = 0$ for each i, which says $a_i = 0$ or $i = 0$ in F. In other words, $a_i = 0$ unless $p|i$ and then we can write

$$f(x) = \sum_{i=0}^{m} a_{ip} x^{ip}.$$

But σ is surjective, then $a_i p = (\alpha^i)^p$ for some $\alpha_i \in F$ for each i and

$$f(x) = \sum_{i=0}^{m} (\alpha_i)^p x^{ip} = (\sum_{i=1}^{m} \alpha_i x^i)^p.$$

This polynomial is definitely reducible and we reach a contradiction. □

This theorem says that fields of characteristic 0 and finite fields are perfect. There is actually a more elementary proof when $F = \mathbb{F}_p$.

Theorem 2.4.5. *Let $f(x) \in \mathbb{F}_p[X]$ be irreducible and of degree n. Then f is irreducibility and f divides $X^{p^n} - X$. (Hence or otherwise, $X^{p^n} - X$ has a factorization $X^{p^n} - X = \prod_{d|n} \prod_{f_d} f_d$, where f_d runs over all irreducible polynomials of degree d.)*

Sketch of proof. Assume $f(X) \neq X$ and the image of X is $x \in \mathbb{F}_p[X]/(f) = E$. Then $[E : \mathbb{F}_p] = n$ and $|E| = p^n$. We then know $E^\times$ is cyclic of order $p^n - 1$ and then $x^{p^n - 1} = 1$ and $x^{p^n} = x$. So $X^{p^n} - X$ has a root x and then $f \mid X^{p^n} - X$ by Theorem 1.2.10. Moreover, $X^{p^n} - X$ has no repeated roots — its has at most p^n roots and they are all of E. □

Definition 2.4.6. Let E/F be an algebraic extension of fields, and let $\alpha \in E$ be algebraic over F. We say that α is *separable* over F if the minimal polynomial of α over F is separable. We say that E/F is *separable* if every element of E is separable over F.