

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 $1, X, X^2, \dots, X^n, \dots$, with the multiplication

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

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. $\deg(f + g) \leq \max(\deg f, \deg g)$,
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 in $\mathbb{Q}[X]$.*

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 $i = 0, 1, \dots, n-1$,
3. $p^2 \nmid a_0$.

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

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 $F[X]/(f)$ is a field.*

Theorem 1.1.9. *Any ring homomorphism between two fields is injective.*

One sentence proof: there is no non-trivial proper ideal in 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 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 $F \not\subseteq E$, as long as there is an obvious embedding of F into E (an embedding is a homomorphism which 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 $[E : F] = \infty$.

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 $\{1, x, x^2, \dots\}$ 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 . \square

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 root of $x^2 - 3 \in E[x]$ (so $1, \sqrt{3}$ form a E -basis of F), 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 and α a non-zero element in E . Then we have the following:*

1. α is algebraic;
2. there is a unique non-zero monic irreducible polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$, moreover, $\deg(f) \leq [E : F]$;
3. if α is a root of a polynomial $g(x) \in F[x]$, then $f \mid g$;
4. if $I = (f)$, then $F[x]/I \cong F(\alpha)$; indeed, there exists an isomorphism $\phi : F[x]/I \rightarrow F(\alpha)$ with $\phi(x + I) = \alpha$ and $\phi(a + I) = a$ for all $a \in F$;
5. if α' is another root of f (in E), then $F(\alpha) \cong F(\alpha')$

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

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

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

$$c_0 \cdot 1 + c_1 \alpha + \dots + c_{[E:F]} \alpha^{[E:F]} = 0.$$

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

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

where one may consider it as the restriction of $e_\alpha : E[x] \rightarrow E$. 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 kernel and hence 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, $\text{im}(\varphi)$ is a domain. So the kernel is a prime (hence maximal) ideal and therefore f is irreducible and $\text{im}(\varphi)$ is a field containing \mathbb{Q} and α indeed. ϕ is the canonical isomorphism induced by φ .

Finally, notice both $F(\alpha), F(\alpha')$ are isomorphic to $F[x]/I$. □

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

Remark. In some textbook, the minimal polynomial is denoted by $\text{irr}(\alpha, F)$.

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

Proof. With the knowledge from 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 $f(x) = a_0 + a_1x + \dots + a_{d-1}x^{d-1} + x^d$, where $a_i \in k$ for all i . In $K = k[x]/I$, we have

$$\begin{aligned} p(\beta) &= (a_0 + I) + (a_1 + I)\beta + \dots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \dots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1x + I) + \dots + (x^d + I) \\ &= a_0 + a_1x + \dots + a_{d-1}x^{d-1} + x^d + I \\ &= f(x) + I = 0 + I. \end{aligned}$$

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 $r + I = b_0 + b_1\beta + \dots + b_{d-1}\beta^{d-1}$ if we express $r(x) = b_0 + b_1x + \dots + b_{d-1}x^{d-1}$.

If $\{1, \beta, \beta^2, \dots, \beta^{d-1}\}$ is not linearly independent, then we can find coefficients $c_i \in k$ not all zero such that

$$c_0 + c_1\beta + \dots + c_{d-1}\beta^{d-1} = 0.$$

Define $g(x) \in k[x]$ by $g(x) = \sum_{i=0}^{d-1} c_i x^i$. 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* (of f) 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 $\varphi : F \rightarrow F$ 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 $\text{Aut}(F)$. We say that $\varphi \in \text{Aut}(F)$ fixes X if $\varphi(x) = x$ for all $x \in X$, and we denote the set of automorphisms of F fixing X by $\text{Aut}(F/X)$.

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 $\text{Aut}(F/X)$ is a group under composition.*

Proof. Just straightforward verifications. □

Example 1.3.3. Consider $\text{Aut}(\mathbb{C}/\mathbb{R})$. Every element of \mathbb{C} can be written as $x + yi$ with $x, y \in \mathbb{R}$. For any $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{R})$, 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 $\text{Aut}(\mathbb{C}/\mathbb{R})$ contains exactly two elements: the trivial one and the complex conjugation. It is clear that $\text{Aut}(\mathbb{C}/\mathbb{R})$ 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 $\text{Aut}(E/F)$ 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 $\alpha_1, \dots, \alpha_n \in E$ for E/F . Any element of E can be written uniquely in the form

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

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

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

In other words, the automorphism σ is entirely defined by the n values $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. 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 there 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 $\text{Aut}(E/F)$ is a finite group. Moreover, if we have $E = F(\alpha)$ for some $\alpha \in E$, then $\text{Aut}(E/F)$ 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 $\text{Aut}(E/F)$ (indeed, F need not even be a field). Unfortunately, there are interesting extensions E/F for which the group $\text{Aut}(E/F)$ 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 $\sigma \in \text{Aut}(E/\mathbb{Q})$. 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 $\text{Aut}(E/\mathbb{Q})$ 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 $\text{Aut}(\mathbb{C}/\mathbb{R})$ is that the non-trivial element fixes exactly \mathbb{R} . In the example above, the (trivial) group $\text{Aut}(E/\mathbb{Q})$ 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 $\text{Aut}(\mathbb{R}/\mathbb{Q})$ is also trivial. Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$. 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 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. 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 $\sigma : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ by $\sigma(x) = x^p$. By the binomial theorem, and the fact that p divides the binomial coefficient $\binom{p}{j}$ for any $1 \leq j \leq p-1$, 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 $\mathbb{F}_{p^n}^\times$ 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 $\sigma \in \text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. It's possible to show that σ generates this group (later).

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 possibly larger field containing all the roots). From what we have learnt from last week, we know an element in $\text{Aut}(E/F)$ 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 $\sigma(x) : F \rightarrow F, x \mapsto X$ 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 $1 \leq j < p$. 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, $i a_i = 0$ for each i , which says $a_i = 0$ or $i = 0$ in F . In other words, $a_i = 0$ unless $p \mid i$ and then we can write

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

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

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

This polynomial is definitely reducible and we reach a contradiction. \square

This theorem says that fields of characteristic 0 and finite fields are perfect. One has to work fairly hard to come up with an example of an inseparable extension. But these do come up naturally in algebraic geometry over fields of positive characteristic. Moreover, 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 separable and f divides $X^{p^n} - X$. (Hence or otherwise, $X^{p^n} - X$ has a factorization $X^{p^n} - X = \prod_{d \mid n} \prod_{f_d} f_d$, 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 — it has at most p^n roots and they are all of E . \square

A lot of results about field theory that are valid in characteristic 0 carry over to perfect fields in characteristic p (but not everything), and the reader should be attentive to this point when reading texts which try to make life easy by always assuming fields have characteristic 0. You should always check if the theorems (and even proofs) go through to general perfect fields.

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 .

Theorem 2.4.7. A field K is perfect if and only if every finite extension of K is a separable extension.

Proof. Suppose K is perfect: every irreducible in $K[X]$ is separable. If L/K is a finite extension then the minimal polynomial in $K[X]$ of every element (which is algebraic) of L is irreducible and therefore separable, so L/K is a separable extension.

Now suppose every finite extension of K is a separable extension. To show K is perfect, let $f(X) \in K[X]$ be irreducible. Consider the stem field $L = K(\alpha)$ from Theorem 1.2.12, where $f(\alpha) = 0$. This field is a finite extension of K , so a separable extension by hypothesis, so α is separable over K . Since $f(X)$ is the minimal polynomial of α in $K[X]$, it is a separable polynomial. \square

It is clear that extensions of fields of characteristic 0 have characteristic 0, and that finite extensions of finite fields are finite, so this theorem is only non-trivial if F is infinite, but has a positive characteristic.

Theorem 2.4.8. Let L/K be a finite extension and say $L = K(\alpha_1, \dots, \alpha_n)$. Then L/K is separable if and only if each α_i is separable over K .

Let's postpone the proof till we introduce Galois group. The usefulness of this theorem is that it gives a practical way to check a finite extension L/K is separable: rather than show every element of L is separable over K it suffices to show there is a set of field generators for L/K that are each separable over K .

Example 2.4.9. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is separable.

A possible term paper may discuss (purely) inseparable extensions, those field extensions over the function fields.

2.5 The primitive element theorem

In this section we prove a result which is not entirely necessary for the discourse, but simplifies the proofs of several other theorems.

Definition 2.5.1. A field extension E/F is *primitive* if there is an element $\alpha \in E$ such that $E = F(\alpha)$.

Example 2.5.2. We already show $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is primitive.

Theorem 2.5.3 (Primitive Element Theorem). *Let E/F be a finite, separable extension of fields. Then E/F is a primitive extension,*

Proof. We will first note that the theorem is trivial if F is a finite field, since in this case E is also finite, and E^\times is a cyclic group. Any generator α will clearly satisfy $E = F(\alpha)$.

We also note that it suffices to prove the theorem in the case $E = F(\alpha, \beta)$, since the general case follows by induction (E will always have some finite basis over F). So we'll suppose that F is infinite and that $E = F(\alpha, \beta)$ for some $\alpha, \beta \in E$. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of the minimal polynomial $f(x)$ of α over F , and $\beta = \beta_1, \beta_2, \dots, \beta_m$ the roots of the minimal polynomial $h(x)$ of β over F . All the roots are distinct since E is separable. Since F is infinite, we may choose some $a \in F$ such that

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

for any i and any $j \neq 1$. Let $\gamma = \alpha + a\beta$

Claim: $F(\alpha, \beta) = F(\gamma)$.

The theorem follows from the claim (and induction) immediately.

Proof of Claim: Note that since $\gamma = \alpha + a\beta$, we have $F(\alpha, \beta) = F(\gamma, \beta)$. It is enough to show β is in $F(\gamma)$. Let $g(x) = f(\gamma - ax) \in F(\gamma)[x]$. Note that

$$g(\beta) = f(\gamma - a\beta) = f((\alpha + a\beta) - a\beta) = f(\alpha) = 0.$$

On the other hand, we cannot have $g(\beta_j) = 0$ for $j \neq 1$, as $f(\gamma - a\beta_j) = 0$ would imply $\gamma - a\beta_j = \alpha_i$ for some i . Substituting $\gamma = \alpha + a\beta$ inside, we reach at

$$a(\beta - \beta_j) = \alpha_i - \alpha.$$

This contradicts to our initial assumption about a . Thus $\gcd(g(x), h(x)) \in F(\gamma)[x]$ has exactly one root, namely $x = \beta$. And since $h(x)$ has no repeated root, neither does $\gcd(g(x), h(x))$. It follows that $\gcd(g(x), h(x)) \in F(\gamma)[x]$ is a linear polynomial vanishing at β , and in fact $\beta \in F(\gamma)$. (A hidden fact here is that if E/F is a field extension and $g(x), f(x)$ are in $F[x]$, then $\gcd_{F[x]}(g, f) = \gcd_{E[x]}(g, f)$. A simple explanation is that $\gcd(g, f)$ can be computed with the Euclidean algorithm, which operates on the coefficients of g and f and so never leaves F .) \square

The next theorem gives a complete description of field extensions which admit a primitive element.

Theorem 2.5.4 (Steinitz). *Let E/F be a finite extension of fields. Then $E = F(\alpha)$ for some $\alpha \in E$ if and only if there exist only finitely many distinct intermediate fields $F \subset K \subset E$.*

Proof. We have seen that the primitive element property trivially holds in all finite fields, and the property of there only being finitely many intermediate fields does as well. We will suppose, then, that F is infinite. Suppose that there are only finitely many intermediate fields. We will show that $E = F(\alpha)$ for some α , and just as in the proof of Theorem 2.5.3 (which is very similar) we are free to suppose that $E = F(\beta, \gamma)$. Consider the fields $F(\beta + a\gamma)$, for $a \in F$. Since all of these fields lie between F and E , there must be distinct $a_1 \neq a_2 \in F$ with $F(\beta + a_1\gamma) = F(\beta + a_2\gamma)$. Now, since $\beta + a_1\gamma$ and $\beta + a_2\gamma$ are both in this field, so is $(a_2 - a_1)\gamma$, and hence γ (since $a_2 - a_1 \neq 0$).

It follows $\beta = (\beta + a_1\gamma) - a_1\gamma$ is in $F(\beta + a_1\gamma)$ as well. Thus $E = F(\beta, \gamma) = F(\beta + a_1\gamma)$, and we are done.

For another direction, suppose that $E = F(\alpha)$. For each intermediate field $F \subset K \subset E$, we take $f_K(x) \in K[x] \subset E[x]$ to be the minimal polynomial of α over K . By unique factorization in $E[x]$, each $f_K(x)$ must be a (monic) divisor of $f_F(x)$ (where $f_F(x)$ is considered as a polynomial in $E[x]$), and there are only finitely many of these. It suffices to show, then, that this function $K \rightarrow f_K(x)$ is one-to-one. Let $F(f_K)$ be the field generated over F by the coefficients of $f_K(x)$. Then certainly $F(f_K) \subset K$. On the other hand, $f_K(x)$ is an irreducible monic polynomial with coefficients in $F(f_K)$, which vanishes at α , and so α has degree $\deg(f_K)$ over $F(f_K)$. It follows from the fact that

$$[F(\alpha) : F(f_K)] = [F(\alpha) : K][K : F(f_K)]$$

that $[K : F(f_K)] = 1$. In other words, $K = F(f_K)$, showing that the map is injective. It follows at once that there are only finitely many subfields $F \subset K \subset E$. \square

Remark. Patrick Ingram refers Theorem 2.5.4 as the primitive element theorem. But Rotman labels it after Steinitz. And many textbooks (Rotman included) refers Theorem 2.5.3 as the primitive element theorem instead. We follow Rotman's conventions.

2.6 Algebraic closure

Although we can get by with constructing fields like $\mathbb{Q}(i)$ as quotients:

$$\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2 + 1),$$

it is often useful to think of all of the possible algebraic extensions as being subfields of one large (infinite) extension.

Definition 2.6.1. A field F is said to be *algebraically closed* if every non-constant polynomial $f(x) \in F[x]$ has a root in F or, equivalently, if every polynomial in $F[x]$ factors as a product of linear terms.

Theorem 2.6.2. *Let F be a field. Then there exists a field $\overline{F} \supset F$ which is algebraically closed and algebraic over F . This field is unique up to isomorphism.*

We will not try to prove Theorem 2.6.2 but give a direction here. As you might guess, Zorn's lemma is inevitable in such kind proof. The problem is how to apply it.

One can imagine looking at the "set" of all algebraic extensions of F . This collection of fields is partially ordered under inclusion, and linearly ordered chains in the collection have least upper bounds (their union). If this were a set of fields, then it would follow from Zorn's Lemma that there is a maximal element, call it \overline{F} . This would be an algebraic extension of F : it would have no proper algebraic extension, and hence it would have to be algebraically closed. This is the algebraic closure of F . The problem with this argument is that the collection of algebraic extensions of F is too large to be a set, and hence one cannot apply Zorn's Lemma.

Instead, let's do this. Let P be the set of all non-constant monic polynomials in $F[X]$ and let $A = F[t_f]_{f \in P}$ be the polynomial ring over F generated by a set of indeterminates indexed by P . This is a *huge* ring. For each $f \in F[X]$ and $a \in A$, $f(a)$ is an element of A . Let I be the ideal

in A generated by the elements $f(t_f)$ as f runs over P . The first step is to show I is proper and hence contained in a maximal ideal \mathfrak{m} . The next step is then to show A/\mathfrak{m} is algebraically closed. The last step is to show the algebraic closure is unique up to isomorphism.

Theorem 2.6.3. *Let F be a field, \overline{F} its algebraic closure, and let $F \subset E \subset \overline{F}$ be a finite separable extension of F . Then there are precisely $[E : F]$ distinct embeddings $E \rightarrow \overline{F}$ which fix F .*

Proof. By the primitive element theorem, we may suppose that $E = F(\alpha)$, and let $f(x) \in F[x]$ be the minimal polynomial of α . For each root $\alpha' \in \overline{F}$, we have an isomorphism

$$E = F(\alpha) \cong F(x)/(f(x)) \cong F(\alpha') \subset \overline{F}.$$

This gives us $\deg(f) = [E : F]$ embeddings of E into \overline{F} , which must be distinct, since they send α to the $\deg(f)$ distinct roots of f (hidden here is the fact that E/F is separable). On the other hand, any embedding $F(\alpha) \rightarrow \overline{F}$ which fixes F is determined entirely by the value at α (which must be a root of the same minimal polynomials in $F[x]$ as α), and so these are the only possible embeddings of $E \rightarrow \overline{F}$. \square

Corollary 2.6.4. *Let $E=F$ be a finite separable extension. Then*

$$|\text{Aut}(E/F)| \leq [E : F].$$

Proof. Each distinct automorphism $\sigma \in \text{Aut}(E/F)$ gives a distinct embedding $\sigma : E \rightarrow E \subset \overline{F}$, which fixes F . \square

Week 3

3.7 Splitting fields

Definition 3.7.1. A *splitting field* of the polynomial $f(x) \in F[x]$ is a field extension E/F such that $f(x)$ factors into linear terms in $E[x]$, namely,

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n),$$

and such that $E = F(\alpha_1, \dots, \alpha_n)$.

This is, the splitting field is the smallest field (unique up to isomorphism) extension containing all the roots of $f(x)$. If f is irreducible and separable, the all linear terms above are distinct. This may not be true if f is inseparable.

Example 3.7.2. Let $f(x) = x^3 - 2 \in \mathbb{Q}[Z]$. $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of f , since it does not contain all the root. The splitting field is $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ where ω is a third of unity, in other words, $1, \omega, \omega^2$ are roots of $x^3 - 1$. Note that we also have $E = \mathbb{Q}(\omega, \sqrt[3]{2})$. The symbol $\sqrt[3]{2}$ is ambiguous, but we can either take the real cube root, or simply note that any choice defines the same field (only now that we've thrown in ω).

The following theorem, which is perhaps surprising, says that the splitting field of a polynomial contains a splitting field for the minimal polynomial of any element of that field.

Theorem 3.7.3. Let E/F be a finite extension of fields. The following are equivalent:

1. E is the splitting field of some polynomial over F ;
2. every irreducible polynomial $g(x) \in F[x]$ with a root in E factors completely over E ;
3. any embedding $\sigma : E \rightarrow \overline{F}$ fixing F is an automorphism of E , namely, $\text{im}(\sigma) = E$.

We need a technical lemma to prove Theorem 3.7.3.

Lemma 3.7.4. Let E/F be a finite extension. Suppose that $F' \subset E$ is a field and that there is a embedding $\psi : F' \rightarrow \overline{F}$ fixing F . Then ψ can be extended to an embedding $\phi : E \rightarrow \overline{F}$ in the sense that $\phi|_{F'} = \psi$.

Proof. We proceed by induction on $[E : F']$. If $[E : F'] = 1$, then $E = F'$ and we are done.

Suppose that $[E : F'] > 1$ and that the statement is true for fields $F \subset F'' \subset E$ with $[E : F''] < [E : F']$. Since $E \neq F'$, there is an element $\beta \in E \setminus F'$ which, necessarily, is algebraic

over F' . Now we have been given an embedding $\psi : F' \rightarrow \overline{F}$ which fixes F . For a polynomial $g(x) \in F'[x]$, we let $g^\psi(x) \in \overline{F}$ be the polynomial obtained by applying ψ to each coefficient. Then clearly $g(x) \rightarrow g^\psi(x)$ is an isomorphism from $F'[x]$ to $K[x]$, where $K \subset F$ is the image of F' under ψ . Now, if $g^\psi(\beta') = 0$, it follows easily that

$$F'(\beta) \cong F'[x]/(g) \cong K[x]/(g^\psi) \cong K(\beta').$$

This gives an embedding of $\psi' : F'(\beta) \rightarrow F$ which extends ψ . Since $[E : F'(\beta)] < [E : F']$ (because $[F'(\beta) : F] > 1$), we may apply the induction hypothesis to $\psi' : F'(\beta) \rightarrow E$, and conclude that it extends to an embedding $E \rightarrow \overline{F}$. \square

Proof of Theorem 3.7.3. We show that

$$(3) \implies (2) \implies (1) \implies (3).$$

(2) \implies (1): For a primitive extension $E = F(\alpha)$, E is the splitting field of the minimal polynomial of α over F . If $E = F(\alpha_1, \dots, \alpha_n)$, the E is the splitting field of the products of the minimal polynomials of α_i over F for $i = 1, \dots, n$.

(3) \implies (2): Let $g(x) \in F[x]$ be an irreducibility polynomial with a root $\beta \in E$. For each root $\beta' \in \overline{F}$, we obtain an embedding: $F(\beta) \rightarrow \overline{F}$ with $\phi(\beta) = \beta'$. (Indeed, both $F(\beta), F(\beta')$ are isomorphic to $F[x]/(g)$ by Theorem 1.2.10.) By Lemma 3.7.4, we can extend to an embedding $\sigma : E \rightarrow \overline{F}$ (fixing F). The image of σ is E by assumption. In other words, $\beta' = \phi(\beta)$ is in E . As β' runs over all possible roots, E contains all the roots of g and so g factors completely in $E[x]$.

(1) \implies (3): Let E be the splitting field of $f(x) \in F[x]$ and $\sigma : E \rightarrow \overline{F}$ an embedding fixing F . We know that σ permutes the roots of $f(x)$ in \overline{F} , so the image of σ contains all the roots of f . But E is exactly generated by the roots of f , so the $\text{im}(\sigma)$ is as well. It follows that $\sigma(E) = E$. \square

Definition 3.7.5. A finite extension E/F is *normal* if it satisfies any of the equivalent conditions in Theorem 3.7.3.

There is an alternate characterization of normal extensions in the separable case:

Theorem 3.7.6. Let E/F be a finite separable extension. The E/F is normal if and only if

$$|\text{Aut}(E/F)| = [E : F].$$

Proof. Suppose that E/F is normal. We know that $\text{Aut}(E/F) \leq [E : F]$ by Corollary 2.6.4, since each element of $\text{Aut}(E/F)$ defines an embedding $E \rightarrow \overline{F}$ fixing F . On the other hand, each such embedding is an automorphism of E by the above theorem, and there are $[E : F]$ of these. That implies $[E : F] \leq |\text{Aut}(E/F)|$.

On the other hand, if $|\text{Aut}(E/F)| = [E : F]$, then each of the $[E : F]$ embeddings must give rise to an automorphism, since $\text{Aut}(E/F)$ is just the number of these embeddings under which the image of E is E . So $|\text{Aut}(E/F)| = [E : F]$ implies E/F is a normal extension. \square