Coursera - Introduction to Galois Theory

Ekaterina Amerik

February 22 2016

Contents

Chapter 1

Generalities on algebraic extensions

Ekaterina Amerik is working at the mathematical department of Higher School of Economics.

This is a course about field extensions and we assume familiar the basic notions of abstract algebra, like groups, rings, fields, modules, ideals, and their basic properties. We also assume a certain knowledge of linear algebra. All rings we consider will be commutative, associative, and with unity.

1.1 Field extensions: examples

Definition K, L fields. L is said to be an **extension** of K, if K subfield of L.

An equivalent definition is:

Definition L is an **extension** of K if L is a K-algebra.

A K-algebra A is a ring with a structure of a K-module such that these two structures are compatible: the multiplication $A \times A \to A$ is K-bilinear, $(k_1a_1)(k_2a_2) = k_1k_2a_1a_2$, where $k_i \in K$, $a_i \in A$.

Why is a field containing K as a subfield the same thing as a K-algebra?

Defining a K-algebra structure on A is the same as defining a homomorphism of rings $f : K \to A$. Given a K-algebra, we can define a homomorphism $f(k) = k \cdot 1$. And conversely, if I have a homomorphism of rings $f : K \to A$, I can define a K-algebra structure by setting $ka = f(k) \cdot a$.

If A is a field L, then any homomorphism $f : K \to L$ is injective. There are several ways to see this. 1) $f(k)$ is always invertible: $1 = f(1) =$

$f(kk^{-1}) = f(k)f(k^{-1})$. So $f(k) \neq 0$ if $k \neq 0$. In particular f is injective. 2) Ker f is always an ideal: a field does not have nontrivial ideals, the only ideals are (0) and $(1) = K$.

If you don't know this, you are strongly encouraged to do it as an exercise.

Example $\mathbb{C}$ is an extension of $\mathbb{R}$. And $\mathbb{R}$ is an extension of $\mathbb{Q}$.

Example Any field has what is called a characteristic, so if L is a field, there are two possibilities:

1) If you take the unit element and start adding it to itself, you never obtain $1 + 1 + \cdots + 1 \neq 0$. In this case, we say that the char $K = 0$. And we see that in this case of course, $\mathbb{Z} \subset L \implies \mathbb{Q} \subset L$. So L is an extension of $\mathbb{Q}$.

2) Or, if you take the unit element and start adding it to itself, you obtain 0 at certain point $\sum_{m \text{ times}} 1 = 0$. The minimal m with this property is prime. m is the **characteristic** of this field. Then L does not contain $\mathbb{Z}$, it contains $\mathbb{Z}/p\mathbb{Z}$. For p prime $\mathbb{Z}/p\mathbb{Z}$ is a field. To emphasize its field structure we denote it by $\mathbb{F}_p$. L is an extension of $\mathbb{F}_p$.

One calls $\mathbb{Q}$ and $\mathbb{F}_p$ the prime fields. They don't contain any proper subfields.

Any field is an extension of one prime field.

This example is very important:

Example So let's take the ring of polynomials in one variable over K. And let's consider the quotient ring by an ideal generated by an irreducible polynomial P: $K[x]/(P)$. Then $K[x]/(P)$ is a field.

There are two ways to see these.

Way 1. If Q is a polynomial which is not a multiple of P ($Q \notin (P)$), then Q is prime to P ($gcd(Q, P) = 1$). And then you have the Bézout identity. $\exists A, B \in K[x]$, such that $AP + BQ = 1$, so what you see is that $BQ = 1 \bmod P$, and therefore B is an inverse of Q in $K[x]/(P)$.

1.2 Algebraic elements. Minimal polynomial

So let me continue with my third example.

Example *(continued)* **Way 2.** Instead of writing down the Bézout equality, one can also say that an ideal generated by an irreducible element of $K[x]$, (P), is a maximal ideal. And the quotient by a maximal ideal is always a field.

But of course the proof of this amounts to the same Bézout equality. How do you prove (P) is a maximum ideal? You just consider some potentially bigger ideal, that is to say containing P and some element Q not belonging to the ideal generated by P. This Q is going to be prime with P, you can write the Bézout equality and it is in this way that you see that such an ideal will be necessarily equal to the polynomial ring $K[x]$.

So this is an extension of K in an obvious way. Or it's an extension of K because it's a K-algebra, hence an extension of K.

Here a more concrete example.

Example Let's take K equal to the field of two elements. So $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. We have $1 + 1 = 0$. Let us take $P = x^2 + x + 1$, this is an irreducible polynomial over $\mathbb{F}_2$. Then $K[x]/(P)$ is a field of four elements. $K[x]/(P) = \{0, 1, \bar{x}, \overline{x+1}\}$. $\bar{x}$ is the class of x modulo P. And you see that $\bar{x}^2 = -\bar{x} - 1$ since you know that $x^2 + x + 1 = 0$ in our field.

Well, the characteristics of $\mathbb{F}_2$ is 2, so $-1 = 1$, so it's just $\overline{x+1}$, in the same way $(\overline{x+1})^2 = \bar{x}$, and they are inverse of each other: $\bar{x} \cdot \overline{x+1} = 1$.

So this is the structure of a field of four elements. The cardinality of $K[x]/(P)$ is $|K[x]/(P)| = 4$. One writes then $K[x]/(P) = \mathbb{F}_4$. Well, this might be strange at the first sight, because we only know that $K[x]/(P)$ has four elements. And if you write $\mathbb{F}_4$ you somehow mean that there is only one field of four elements. Well, it is true, there is only one field of four elements. In fact, all finite fields of the same cardinality are isomorphic, and we will see it very shortly.

Definition Let L be an extension, $K \subset L$, and $\alpha \in L$. α is **algebraic**, if $\exists P \in K[x]$ such that $P(\alpha) = 0$. Otherwise α is **transcendental**.

Lemma 1.2.1. If α is algebraic then there exists a unique monic polynomial P of minimal degree with this property. Such a polynomial is irreducible. Any other polynomial Q such that $Q(\alpha) = 0$ is divisible by P.

Definition Such a P is called the **minimal polynomial** of α over K. We write $P_{\min}(\alpha, x)$.

Proof. The proof is a direct consequence of definitions. We know that $K[x]$, the polynomial ring in one variable, is a principal ideal domain. And the polynomials vanishing in α, $I = \{Q \in K[x] | Q(\alpha) = 0\}$, certainly form an ideal. So this ideal is generated by one element P, $I = (P)$. P is certainly unique up to a constant element of minimal degree in I. Furthermore, if P was not irreducible, $P = Q \cdot R$, then $P(\alpha) = Q(\alpha) \cdot R(\alpha)$. So $Q(\alpha)$ or $R(\alpha)$ must be 0, which is a contradiction with the minimality to the degree. □

1.3 Algebraic elements. Algebraic extensions

We introduce an important notation.

Definition Let L be an extension of K, $K \subset L$, and $\alpha \in L$. We write $K(\alpha)$ for the smallest subfield of L containing K and α. We write $K[\alpha]$ for the smallest subring or K-algebra containing K and α.

Well, let me give you an example.

Example Well, first of all let me say that $K[\alpha]$ is generated as a vector space over K by 1, α, α^2, $\cdots$, α^n, $\cdots$. So, let me give you an example. $\mathbb{C} = \mathbb{R}(i)$ as a field. But also to $\mathbb{C} = \mathbb{R}[i]$ as a ring. Because any element $z \in \mathbb{C}$ is $z = x + iy$ where x is a real part and y is the imaginary part. So, of course this is a vector subspace generated by 1 and i.

And this is a general phenomenon. So:

Proposition 1.3.1. The following conditions are equivalent (TFAE):

1. α is algebraic over K
2. $K[\alpha]$ as a ring is a finite dimensional vector space over K
3. $K[\alpha]$ as a ring is equal to $K(\alpha)$ as a field.

.

Proof. (1) $\Longrightarrow$ (2). If α is algebraic, then

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0 \text{ where } a_i \in K. \tag{1.1}$$

This is just $P(\alpha)$, where P is a minimal polynomial. So, we see that

$$\alpha^d = -\sum_{i=0}^{d-1} a_i\alpha^i. \tag{1.2}$$

So, you see that α^d, α^{d+1} and so on are going to be linear combinations of the lower powers of α. This implies of course that $K[\alpha]$ is generated by 1, α, $\cdots$, α^{d-1} over K.

And in particular it is finite dimension.

(2) $\Longrightarrow$ (3). It is enough to prove that $K[\alpha]$ is a field. Since, of course, $K[\alpha] \subset K(\alpha)$.

Well, how do you prove this? It is very simple. Well, I'll let $x \in K[\alpha]$. I want to show that this is invertible. Consider the multiplication by x

$(K[\alpha] \to K[\alpha])$. This is a homomorphism of vector spaces, this is an injection of vector spaces over K. But, we know from linear algebra that if you have an injection of finite dimensional vector spaces of the same dimension, then it is also a surjection. Since $K[\alpha]$ is final dimensional this is a surjection. So there exist a $y \in K[\alpha]$, such that $y \cdot x = 1$. So, x is invertible and $K[\alpha]$ is a field. Of course, I have forgotten to say that x was supposed to be nonzero in order to have the multiplication by x injective. But, I guess everybody has understood. So, we were assuming $x \neq 0$ from the beginning.

(3) $\implies$ (1). So if $K[\alpha]$ is a field, then α is algebraic. This is maybe the easiest part. So, if α is not algebraic, then $\nexists P$ such that $P(\alpha) = 0$. But what does this mean? This means that a natural homeomorphism, $i : K[x] \to L$, $P \mapsto P(\alpha)$ is injective. But, $K[x]$ is not a field. And the image of this homeomorphism is $\mathrm{Im}(i) = K[\alpha]$ which is a field. So, this is a contradiction. □

Definition L an extension of K is called **algebraic** over K, if $\forall \alpha \in L$, α is algebraic.

Some properties of those algebraic extensions:

Proposition 1.3.2. If L is algebraic over K, any K-subalgebra L' of L is a field.

Proof. Let's take $L' \subset L$ a subalgebra. Fix an $\alpha \in L'$. I have to show that it's invertible. Well, I know it's algebraic. And then I know that $K[\alpha]$ – which is also subalgebra of L – is a field. And then I know that α is invertible. And since I can do it for any $\alpha \neq 0$, it follows from this, that L' is a field. □

Well, another proposition, which will be important is as follows:

Proposition 1.3.3. Let's have $K \subset L \subset M$. If $\alpha \in M$ is algebraic over K, then it's algebraic over L, and it's minimal polynomial over L divides it's minimal polynomial over K.

$$P_{\min}(\alpha, L) | P_{\min}(\alpha, K)$$

Proof. Well, this is of course clear since I can just consider $P_{\min}(\alpha, K)$ as an element of $L[x]$. □

1.4 Finite extensions. Algebraicity and finiteness

Definition L is said to be a finite extension of K, if it is a **finite dimensional** K-vector space. The dimension of L over K is called the **degree of the extension**. Notation: $\dim_K L = [L : K]$.

Theorem 1.4.1. Suppose L is an extension of K and M is an extension of L, $K \subset L \subset M$. Then M is finite over K if and only if M is finite over L and L is finite over K.

Moreover, in this case the degrees multiply. $[M : K] = [M : L] \cdot [L : K]$.

Proof. Let me prove this theorem for you. One direction: suppose M is finite over K. Well, any family $m_1, \cdots, m_n \in M$ which are linearly independent over L of course is linearly independent over K. [This is obvious because what is linear independence of this is non-existence of linear combinations, of linear combinations with coefficients from L or from K, which is zero. Of course, if there is no such combination with L coefficients a fortiori, there is no such combination with K coefficients because $K \subset L$.]

So, thus, the $\dim_L M$ is finite because you cannot have a linear independent family of more than $\dim_L M < \infty$.

Well, now, on the other hand, L is a K-vector subspace of M. So if M is finite-dimensional over K, then L is also finite dimensional over K since the subspace of a finite dimensional vector space is also finite dimension.

So one direction is easy. The other direction is also easy, but one must make a little computation. So let $e_1, ..., e_n$ be an L-basis of M and let ϵ_1, ..., ϵ_d be a K-basis of L.

So, let us prove that $e_i\epsilon_j$ form a K-basis of M. Well indeed, $\forall x \in M$ is a linear combination of e_i with L coefficients. $x = \sum_{i=1}^n a_i e_i$, $a_i \in L$. Well, each a_i is also a linear combination. Let's say, $a_i = \sum_{j=1}^d b_{ij}\epsilon_j$, $b_{ij} \in K$. So we can write $x = \sum_{i,j} b_{ij}\epsilon_j e_i$. That is to say that $\epsilon_j e_i = e_i epsilon_j$, generate M over K.

And we only have to check that these are linearly independent over K. If $\sum_{i,j} c_{ij} e_i \epsilon_j = 0$, then of course we can recompose the terms. Then we have $\sum_i (\sum_j c_{ij}\epsilon_j) e_i = 0$, where $\sum_j c_{ij}\epsilon_j \in L$. But e_i form a basis, so $\forall i$, $\sum_j c_{ij}\epsilon_j = 0$. But this means – as ϵ_j form a basis – that $c_{ij} = 0$, $\forall i, j$. So the theorem is proved. □

Definition Notation: Let $K(\alpha_1, \cdots, \alpha_n) \subset L$ be the smallest subfield of L containing K and the α_i. I will also often say that this is generated by $\alpha_1, ..., \alpha_n$ over K.

Theorem 1.4.2. *L is finite over K if and only if L is generated by a finite number of algebraic elements over K.*

Proof. Well again, one direction is obvious. If L is a finite dimensional K-vector space, then we can take a K-basis $\alpha_1, \cdots, \alpha_d$. Then L is certainly equal to the smallest subring of L containing $\alpha_1, \cdots, \alpha_d$, which is a field, so it is also a smallest subfield of L containing α_i.

$$L = K[\alpha_1, \cdots, \alpha_d] = K(\alpha_1, \cdots, \alpha_d). \tag{1.3}$$

Now, all α_i are algebraic, this is just because, well moreover, each $K[\alpha_i]$ is a finite dimensional K-algebra, since it is a subring of L which is already finite-dimensional. So then by proposition 1.3.1, α_i is algebraic.

Well, in the other direction it is also not difficult. We have $K[\alpha_1]$ is finite dimensional over K, $K[\alpha_1, \alpha_2]$ is finite dimensional over $K[\alpha_1]$, and so on. In general $K[\alpha_1, \cdots, \alpha_d]$ is finite dimensional over $K[\alpha_1, \cdots, \alpha_{d-1}]$.

All of those elements are algebraic so all $K[\alpha_1, ..., \alpha_i]$ are fields. So $K[\alpha_1, ..., \alpha_i] = K(\alpha_1, ..., \alpha_i)$. And now, just use theorem 1.4.1 to conclude that L which is $K(\alpha_1, ..., \alpha_d)$ is finite over K. □

1.5 Algebraicity in towers. An example.

Algebraic extensions satisfy a similar property to that of finite extensions. If you have a tower of algebraic extensions, then it is algebraic if and only if each floor of this tower is algebraic.

Theorem 1.5.1. *Well, again let L be an extension K, and M an extension of L, $K \subset L \subset M$. Then M is algebraic over K if and only if M is algebraic over L and L is algebraic over K.*

Proof. So, one direction: let $\alpha \in M$. Of course, if it satisfies a polynomial relation with coefficients from K, if $P(\alpha) = 0$, for some $P \in K[x]$ then also, this $P \in L[x]$. So α is algebraic over L. And if now $\alpha \in L$ – we want to prove that it's algebraic over K– then also $\alpha \in M$, and so α is algebraic over K. And so L is algebraic over K.

Another direction. So, I have L, which is algebraic over K and M algebraic over L. I must prove that M is algebraic over K. So, take $\alpha \in M$ and consider the minimal polynomial $P_{\min}(\alpha, L)$. Its coefficients are elements of L, so they are algebraic over K. By the previous theorem, theorem 1.5.1, they generate an extension E which is finite over K. Now, $E(\alpha)$ is also finite over K since $E(\alpha)$ is finite over E. And this means that α is algebraic over K because – since $E(\alpha)$ is finite over K – there will be some linear dependence between the powers of α. □

Okay, let me give you an example.

Example So consider the extension obtained from $\mathbb{Q}$ by adjoining, let's say, $\sqrt[3]{2}$ and or $\sqrt{3}$, that is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. This is clearly algebraic and finite over $\mathbb{Q}$. And what is it's degree? The degree of this extension is 6, indeed, we have

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}). \tag{1.4}$$

$P_{\min}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$. This is an irreducible polynomial over $\mathbb{Q}$, which has the $\sqrt[3]{2}$ as a root. And so $\mathbb{Q}(\sqrt[3]{2})$ is generated over $\mathbb{Q}$ by linearly independent elements: 1, $\sqrt[3]{2}$, and $(\sqrt[3]{2})^2$. So, the degree of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is equal to 3, $\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3$.

Now, $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$. Well, maybe the easiest way to see it is as follows: because otherwise, one would have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2})$. But $\big[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\big] = 2$ has to divides $\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3$. (We have seen that the degrees multiply in towers of finite extensions.) So this is impossible. Therefore $x^2 - 3$ is irreducible over our extension $\mathbb{Q}(\sqrt[3]{2})$, and $x^2 - 3 = P_{\min}(\sqrt{3}, \mathbb{Q}(\sqrt[3]{2}))$.

And the degree of our big extension $\big[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})\big] = 2$. Therefore $\big[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}\big] = 2 \cdot 3 = 6$.

Well, I should have said this earlier. This fact is completely general that the degree of an extension generated by an algebraic element α over K is equal to the degree of the minimal polynomial of α.

Proposition 1.5.2. $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$ if α is algebraic.

Proof. I should have said this earlier, that the proof is obvious. Since we have already remarked several times that $K(\alpha)$ is generated by $1, \alpha, \cdots, \alpha^{d-1}$, where $d = \deg P_{\min}(\alpha, K)$. And in fact this is a basis, independent. □

Well in any case this is a good practical tool to compute the degree of finite extension. And I would like to finish with the little remark which might be helpful to understand the next lecture. So a proposition:

Proposition 1.5.3. Let $K \subset L$ be a field extension. So consider $L' \subset L$, formed by all elements algebraic over K. Then L' is a subfield of L.

Definition One calls it the *algebraic closure* of K in L.

Proof. Well, the proof is, of course, easy. If α and β are algebraic over K, we have to prove that $\alpha + \beta$ and $\alpha \cdot \beta$ are algebraic. But this is trivial by theorem 1.5.1, since $\alpha + \beta, \alpha \cdot \beta \in K[\alpha, \beta]$ which is a finite (by theorem 1.5.1) extension of K. □

1.6 A digression: Gauss lemma, Eisenstein criterion.

Let me summarize what we have done up till now.

- K field, then α is algebraic over K, if root of $P \in K[x]$ (K[x] are the polynomials with coefficients in K).
- L algebraic over K, if $\forall \alpha \in L$ algebraic over K.
- F finite over K, if $\dim_K L < \infty$ (finite dimensional K-vector space).
- Finite $\implies$ algebraic.
- Finite $\iff$ algebraic and finitely generated.
- $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$ (We generate L by a single element α)

So, given some algebraic element over K, a root of some polynomial, it is important to be able to decide whether this is the minimal polynomial of α over K. That is to say, it is important to have some *irreducibility criteria*, and this is something you probably already know. But since it's so important, I would like to remind a couple of things about this.

So how to decide, that a polynomial is irreducible over K? Well in our example, we had a very simple polynomial. So $x^3 - 2$ was irreducible over $\mathbb{Q}$ since it's a cubic polynomial, so if it was not irreducible it would have a root in $\mathbb{Q}$. So this is easy since the degree is equal to 3 and there is no root. But, well, if you ask the question whether $x^{100} - 2$ is irreducible or not, this is already not so simple, right? Well, this is irreducible. And here are a couple of facts which help to see this easily.

Fact 1 (Gauss Lemma). If P decomposes nontrivially. By this I mean P is a product of two factors of strictly smaller degree over $\mathbb{Q}$ (that is $P = Q \cdot R$, where $\deg Q$, $\deg R < \deg P$, or the same is to say that $0 < \deg Q$, $\deg R$), then it is also the case over $\mathbb{Z}$. Well, of course I have to say that I am considering a polynomial with integral coefficients. Well, let me give a proof. So, over $\mathbb{Q}$ write $P = Q \cdot R$. They are not integral, but of course you can multiply by a common denominator, and they become integral. So lets say $mQ = Q_1 \in \mathbb{Z}[x]$ and $nR = R_1 \in \mathbb{Z}[x]$. Then we have $mnP = Q_1R_1$ over $\mathbb{Z}[x]$. Then take $p|mn$. Then modulo p (means over $\mathbb{F}_p$) we have $0 = \overline{Q_1} \cdot \overline{R_1}$ (where bar denotes the reduction modulo p) But we are over $\mathbb{Z}/p\mathbb{Z}$, which is a field, so we have either $\overline{Q_1} = 0$ or $\overline{R_1} = 0$. This means that p divides all coefficients either of Q_1 or of R_1. Say, of Q_1, then we can write $\frac{mn}{p} \cdot P = Q_2 \cdot R_1$

in $\mathbb{Z}[x]$, and here of course $Q_2 = Q_1/p$. Continuing in this way, We arrive at, I don't know, $P = Q_l R_s$ in $\mathbb{Z}[x]$.

Fact 2 (Eisenstein criteria). Let me not prove it in full generality, let me just show this on an example, and then formulate maybe a general criteria. Well how to show that $X^{100} - 2$ is irreducible over $\mathbb{Z}$? This is very easy. We reduce modulo 2, and so if $x^{100} - 2$ decomposes nontrivially as $Q \cdot R$ mod 2 then $x^{100} = \overline{Q} \cdot \overline{R}$ in $\mathbb{F}_2[x]$. This means that $\overline{Q}$ and $\overline{R}$ are of the form x^k, respectively x^l. So they have no constant coefficient modulo two. So the constant coefficient, constant coefficient of both $\overline{Q}$ and $\overline{R}$ is even and this means the constant coefficient of $x^{100} - 2$ must be divisible by 4. And this is not the case.

So the general formulation of Eisenstein's criterion criterion is as follows: In general, if you have a polynomial with integral coefficients $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If $\exists p$ prime such that $p \nmid a_n$, $p | a_i$ for $i \neq n$ and $p^2 \nmid a_0$, then $P \in \mathbb{Z}[x]$ is irreducible. And the proof is exactly the same.

And to conclude, I would like to say that both facts are valid replacing $\mathbb{Z}$ by some unique factorization domain R and replacing $\mathbb{Q}$ by it's fraction field. So, I think this is a good point to finish the first lecture.

Chapter 2

Stem field, splitting field, algebraic closure

2.1 Stem field. Some irreducibility criteria

Consider a polynomial $P \in K[x]$, which is irreducible and monic. Let me give the definition

Definition A *stem field* for P is an extension E of K, such that $\alpha \in E$ root of P, and E is generated by this root $E = K[\alpha]$.

Well, such a thing exists: we can take just $K[x]/(P)$. This is a field, since P is irreducible. Well, on the other hand, any stem field E is isomorphic to such a thing: $E \cong K[x]/(P)$. While it is easier to define the isomorphism in the other direction. Well, let's see, $K[x]/(P) \to E$ by $f \mapsto f(\alpha)$.

Okay. To summarize, we have the following proposition:

Proposition 2.1.1. A stem field exists and if E and E' are two stem fields for $P \in K[\alpha]$, $E = K[\alpha]$, $E' = K[\alpha']$ (α and α' are roots of P), then there exists a unique isomorphism (K-algebras) $E \to E'$, $\alpha \mapsto \alpha'$.

Proof. So existence we have already seen. Uniqueness of the isomorphism: Isomorphism of $K[\alpha]$ with E' is defined by its value on α.

So, what I have to prove still is the existence of such an isomorphism. But this is easy, because I have $\phi : K[x]/(P) \to E$, $x \mapsto \alpha$, and $\psi : K[x]/(P) \to E'$, $x \mapsto \alpha'$. And I just take $\psi^{-1} \cdot \phi : E \cong E'$, $\alpha \mapsto \alpha'$. □

Remarks:

1. In particular if a stem field contains two roots of P, then there exists a unique automorphism of it, taking one to the other.

2. If E is a stem field of an irreducible polynomial, then $[E : K] = \deg P$. And conversely: If $[E : K] = \deg P$ and E contains a root of P then E is a stem field. (Otherwise it's degree would be strictly greater then the degree of P.)

Now I can give you some more irreducible criteria.

Corollary 2.1.2. $P \in K[x]$ irreducible over K if and only if it does not have roots in extensions L of K of degree $\leq n/2$, where $n = \deg P$.

Proof. Otherwise if P is not irreducible, then it has a prime, irreducible factor Q with $\deg Q \leq n/2$ (where $n = \deg P$) and one can take it's stem field as L.

In the other direction. Conversely, if P has a root $\alpha \in L$, then of course $P_{\min}(\alpha, K)$ divides P. So P cannot be irreducible. □

Okay, one more irreducibility criterion.

Corollary 2.1.3. Let $P \in K[x]$ irreducible, $\deg P = n$. Let L be an extension $\deg L = m$. If $(n, m) = 1$ (n and m are relatively prime), then P is irreducible over L.

Okay, you see, an irreducible polynomial might become reducible over an extension, but it doesn't happen if the degrees are relatively prime.

Proof. If this is not the case $Q|P$ in $L[x]$, let M be a stem field of Q over L. So, we have $K \subset L \subset M = L[\alpha]$. So $K[\alpha]$ (α is a root of Q so it's a root of P), is a stem field of P over K. So $\deg_K K(\alpha) = n = \deg P$.

Well, on the other hand, if $\deg Q = d$, then $[M : L] = d$. And so the total degree $[M : K] = m \cdot d$. But $K[\alpha]$ is a subextension of M. So the degree $n|m \cdot d$. And since $(n, m) = 1$, then, $n|d$, but $d < n$. So, $n = d$ and P is irreducible over L. □

2.2 Splitting field

$P \in K[x]$ not necessarily irreducible.

Definition A *splitting field* of P over K is an extension L, where P is split (i.e. is a product of linear factors) and the roots of P generate L.

It's the smallest field extension where P is split.

Theorem 2.2.1. 1. A splitting field exists and its degree over K is less or equal than $d!$, where $d = \deg P$.

2. (Uniqueness up to an isomorphism.) If L, L' are two splitting fields then they are isomorphic as K-algebras. But such an isomorphism will not necessarily be unique.

Proof. We shall prove this theorem by induction on d. If $d = 1$ everything is trivial. And a splitting field is just K itself. So, let me suppose that $d > 1$, and theorem is proved for all polynomials of degree $< d$ and over any field K. Then we take Q an irreducible factor of P. Let α be a root. So $L_1 = K[\alpha]$ is a stem field of Q. So, over L_1 we have $P = (x - \alpha)R$. And we know that we have a splitting field L of R over L_1 and its degree is at most deg$R! \leq (d-1)$. This will be also a splitting field of P over K. $[L : K] = [L : L_1] \cdot [L_1 : K] \leq (d-a)! \cdot d = d!$

Now it remains to prove uniqueness up to isomorphism. Let L and M be two splitting fields. Now, let β be a root of Q (some irreducible factor of P) in M. Then $K[\alpha] = L_1$ and and $K[\beta]$ are both stem fields for Q. So, we have an isomorphism $\phi : K[\alpha] \to K[\beta]$, $\alpha \mapsto \beta$.

Now $P = (x - \beta) \cdot S$ in $M[x]$. So, where $S = \phi(R)$. So, M is a splitting field of S over $K[\beta]$. M is an extension of $K[\beta]$. But now let's remember that we have also defined a field extension as an algebra. But M is also a $K[\alpha]$-algebra via ϕ. And as such it is a splitting field of R over $K[\alpha]$. Well, I know you have to meditate about this a little bit, but this is true as soon as you view M as a K-algebra. You sort of take this ϕ into account. So by induction we have $K[\alpha]$-isomorphism $L \to M$. And of course we also have a K-isomorphism. □

Remark: The isomorphism between two splitting fields is not unique. A splitting field in particular can have many K-automorphisms. And in fact, the subject of Galois theory is to study this group of automorphisms. Which you will see in a couple of lectures.

2.3 An example. Algebraic closure

Example Let's take the same polynomial $x^3 - 2$ over $\mathbb{Q}$. Its roots are: $\sqrt[3]{2}$, $j\sqrt[3]{2}$, and $j^2\sqrt[3]{2}$, where $j = e^{2\pi i/3}$. The splitting field $L = \mathbb{Q}(\sqrt[3]{2}, j)$.

Now let us find the automorphisms of L. Well, for these let me write two towers. $\mathbb{Q} \subset \mathbb{Q}(j)$ (degree 2) and $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ (degree 3).

And $\mathbb{Q}(j) \subset \mathbb{Q}(j, \sqrt[3]{2})$ (degree 3) and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(j, \sqrt[3]{2})$ (degree 2).

We see that there is a $\mathbb{Q}(j)$-automorphism σ of L taking $\sqrt[3]{2} \mapsto j\sqrt[3]{2}$. Because L is a stem field of $x^3 - 2$ over $\mathbb{Q}(j)$, so there are automorphisms interchanging roots. And there is also a $\mathbb{Q}(\sqrt[3]{2})$-automorphism τ of L taking $j \mapsto j^2$. Since these are two roots of the same minimal polynomial. So

L is a stem field of the minimal polynomial over $\mathbb{Q}$ of $\sqrt[3]{2}$, and there is an automorphism exchanging those roots. So we have a whole group of automorphisms, which is in fact equal to the group of permutations on three elements. Well, the group of automorphisms of L over K is embedded into S_3 (the permutation groups of 3 elements). Because of those automorphisms permute the roots of $x^3 - 2$. In fact, $\mathrm{Aut}(L/K) = S_3$ since those σ and τ already generate S_3.

Let me now talk about algebraic closure.

Definition A field K is *algebraically closed*, if any nonconstant polynomial has a root in K.

This is the same as to say that any nonconstant polynomial splits as a product of linear factors.

Example For example the field of complex numbers has this property. In fact, we will give a proof of this in the future. Shall be proved by almost pure algebraic means.

Definition An *algebraic closure* of K is a field L, which is algebraically closed and algebraic over K.

Theorem 2.3.1. Any field K has an algebraic closure.

Note that I don't say at this point anything about uniqness. Up to isomorphism or whatever. We will treat this later. Now, let's concentrate on existence.

Proof. Proof is a bit weird. How are we going to proceed? So we first construct K_1 such that $\forall P \in K[x]$ has a root in K_1. Well, this is not yet a victory because we don't know whether any polynomial with coefficients in K_1 has a root in K_1. Maybe we have introduced some new rootless polynomials. Then construct K_2 such that $\forall P \in K_1[x]$ has a root in K_2, and so on and so forth. This is the stratagy.

$K \subset K_1 \subset K_2 \cdots \subset K_n \subset \cdots$. Take $\overline{K} = \bigcup K_n$. I claim that $\overline{K}$ is algebraically closed. Indeed, $\forall P \in \overline{K}[x]$, $\exists n$: $P \in K_n[x]$. So it has root in K_{n+1}, so in $\overline{K}$. So, if we learn to construct such K_1, K_2 and so on this will solve the problem. □

2.4 Algebraic closure (continued)

Proof. continued. Construction of K_1. Let S be the set of all irreducible elements of $K[x]$. So S is a very big set. Let $A = K[(X_P)_{P \in S}]$ (One variable X_P for every $P \in S$). Very big polynomial ring. Let $I \in A$ be the ideal generated by all $P(X_P)$, $\forall P \in S$. So what I claim, is that $I \neq A$ is a proper ideal. Well, indeed if not, then I can write $1 \in A$ as $1 = \sum \lambda_i P_i(X_{P_i})$. So these some generators of I. These are elements of A, right? So also some crazy polynomials in crazy variables. But the main point is that this sum is finite. If my ideal contains 1, then 1 is a finite, a linear combination of my generators. Okay. Well, take L a splitting field of $\prod_{i=1}^{n} P_i$ over K. I generate an extension of K by all the roots of all my P_i which were irreducible over K, okay? So let $\alpha_i \in K$ be a root of P_i in K. Then, my A is polynomial ring. And it's very easy to produce a homomorphism of a polynomial algebra to some other algebra. One must just note where one sends the variables. So, $\exists \phi : A \to L$, $X_{P_i} \mapsto \alpha_i$ and $X_P \mapsto 0$ if $P \neq P_i$. (My A is a polynomial algebra.)

Then $\phi(1) = 0$. And $\phi(P_i(X_{P_i})) = P_i(\alpha_i) = 0$. But this cannot happen. $\phi(1)$ must be equal to 1. So, I is an ideal. Then you know how to get a field. So a fact: any ideal, any proper ideal in any commutative associative ring with unity is contained in a maximal ideal m and the quotient A/m is a field. So I just can take $K_1 = A/m$. And then continue in the same way to construct K_2, ... K_3, K_n and so forth. Maybe I should give you some comment on this fact. This is very important, and the technique is very important.

Digression: ideals in a ring. Any proper ideal is contained in a maximal ideal. This is a consequence of what one calls Zorn's lemma, So let me give you the Zorn's lemma. Consider P, not a polynomial anymore, but a partially ordered set. $C \subset P$ is called a chain if it is totally ordered, that is $\forall \alpha, \beta \in C$, $\alpha \leq \beta$ or $\beta \leq \alpha$. Where $\leq$ is our order relation. Zorn's lemma says: if any non-empty chain in a non-empty P has an upper bound (that is an $M \in P$ such that $M \geq x \forall x \in C$, then P has maximal elements. I will not of course prove this Zorn's lemma because you certainly have heard that this is the same thing basically as the axiom of choice or Zermelo's theorem, so this is relevant for set theory, foundations of mathematics, not to algebra and Galois Theory. But, we shall use it to prove that any ideal is contained in a maximal ideal.

Now, let P be a set of proper ideals in A containing I. This is non empty because contains I. And any chain $\{I_\alpha\}_{\alpha \in J}$ has an upper bound. This is just the $\bigcup I_\alpha$. You check that it is an ideal. I'll leave it as an exercise. So, our set P has maximal elements. So, $I \subset M$, M maximal ideal.

And if we have a maximal ideal, if we take a quotient by a maximal ideal, then this is certainly a field. Well, otherwise it would have some proper ideals $a \in A/m$ would generate a proper ideal. And it's preimage under the projection from A to A/m would strictly contain m.

□

2.5 Extension of homomorphisms. Uniqueness of algebraic closure

To sum up we have just proved the existence of an algebraic closure $\overline{K} = \bigcup_{i=1}^{\infty} K_i$. The set of K_i's was a chain $(\cdots \subset K_i \subset K_{i+1} \subset \cdots)$, and each K_i was constructed as follows: It is a field where each $P \in K_{i-1}[x]$ has a root. And we constructed these K_i by considering a huge polynomial ring over K_{i-1} by a suitable maximal ideal. And to construct a maximal ideal we first have constructed a proper ideal and then have used Zorn's lemma to derive a maximal ideal.

Is there any uniqueness result for the algebraic closure? Yes, we have such a result and to prove this I have to prove another theorem.

Theorem 2.5.1 (Extension of homomorphisms)**.** Let take $K \subset L \subset M$ algebraic extensions. K embended in some algebraic closure, $K \subset \Omega$. Then any homomorphism $\phi : L \to \Omega$ extends to a homomorphism $\widetilde{\phi} : M \to \Omega$.

Proof. And the proof is again an application of Zorn's lemma. Apply Zorn to the following set $\xi = \{(N, \psi) : L \subset N \subset M,\ \psi \text{ extends } \phi\}$. So ξ is not empty. Because for instance $(L, \phi) \in \xi$. What is the order? Partially ordered by the following relation: $(N, \psi) \leq (N', \psi')$ if $N \subseteq N'$ (embedded) and ψ' extends ψ $(\psi'|_N = \psi)$.

Now, any chain (N_α, ψ_α) has an upper bound. $\bigcup_\alpha N_\alpha$ is a subextension of M. ϕ defined in the obvious way (for $x \in N_\alpha$, $\psi(x) = \psi_\alpha(x)$). (We take (N, ψ) as an upper bound for our chain.)

So our set ξ has maximal elements. So let (N_0, ψ_0) be one of them. And suppose that $N_0 \neq M$ (strictly included in M). Well, now it's very easy to get a contradiction. Take $x \in M \setminus N_0$ and consider $P_{\min}(x, N_0)$. Let α be a root in Ω (algebraic closure). Then, define $N_0(x) \to \Omega$ by $x \mapsto \alpha$ and ψ_0 on N_0. So this gives a contradiction with maximality of (N_0, ψ_0). But we have found a way to extend it again. So we've got a contradiction, so $N_0 = M$ take $\widetilde{\phi} = \psi_0$. □

Corollary 2.5.2. The algebraic closure is unique up to an isomorphism. If Ω, Ω' are algebraic closures of K then they are isomorphic as K-algebras.

Proof. Since, you have an imbedding of K into Ω and to Ω'. Then you extend i to a map of $\phi : \Omega' \to \Omega$. And, in fact, since you can do it in the other direction as well, you eventually obtain that such a map must be an isomorphous. □

2.6 An example (of extension)

Let me formulate two corollaries of the theorem on extension of homomorphisms.

Corollary 2.6.1. An algebraic closure of K is unique up to an isomorphism of K-algebras.

Corollary 2.6.2. Any algebraic extension of K embeds into the algebraic closure.

Example *Extension of homomorphisms.* Let's take $K = \mathbb{Q}$. And let's fix an algebraic closure, $\overline{\mathbb{Q}}$ (e.g. $\overline{\mathbb{Q}} \subset \mathbb{C}$, the set of algebraic numbers. That is roots of polynomials with rational coefficients).

$L = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2 - 2)$. Let α denote the class of $x \in L$. And L has two embeddings in $\overline{\mathbb{Q}}$. $\phi_1 : \alpha \mapsto \sqrt{2}$ and $\phi_2 : \alpha \mapsto -\sqrt{2}$. ϕ_i are identity on $\mathbb{Q}$. α can go to both roots of the polynomial, $x^2 - 2$.

Now, consider $M = \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}/(y^4 - 2)$. Let β denote the class of $x \in M$. M hat 4 embedding in $\overline{\mathbb{Q}}$. That is $\beta \mapsto \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. $\psi_1 : \beta \mapsto \sqrt[4]{2}$ and $\psi_2 : \beta \mapsto -\sqrt[4]{2}$ extend ϕ_1. M is an extension of L, $M = L[y]/(y^2 - \alpha)$.

$\psi_3 : \beta \mapsto -i\sqrt[4]{2}$ and $\psi_4 : \beta \mapsto i\sqrt[4]{2}$ extend ϕ_2. $\pm i\sqrt[4]{2}$ are the square roots of $-\sqrt{2}$.

Chapter 3

Finite fields. Separability, perfect fields

3.1 Finite fields

We have seen: K finite field $\implies$ char$K = p$, p prime number. K finite extension of $\mathbb{F}_p$, which is a finite dimensional vector space over $\mathbb{F}_p$. If $n = [K : \mathbb{F}_p]$, then the cardinality of K is $|K| = p^n$. Notation: $K = \mathbb{F}_{p^n}$.

Does K exists? Is K unique?

Remark. If char $K = p$, then consider $F_p : K \to K$, $x \mapsto x^p$. This is a field homomorphism: $(x + y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$.

The second properties is true in all fields and the first is particular for characteristic p. Because if you decompose this $(x + y)^p$ by the binomial formula, almost all coefficients will be divisible by p. It is called *Frobenius homomorphism.*

In the same way, $F_{p^n} : x \mapsto x^{p^n}$ is also a field homomorphism.

Theorem 3.1.1. Fix an algebraic closure $\mathbb{F}_p \subset \overline{\mathbb{F}_p}$. A splitting field of $x^{p^n} - x$, the field generated by its roots in $\overline{\mathbb{F}_p}$, has p^n elements. Conversely: Any field of p^n elements is a splitting field of $x^{p^n} - x$. Moreover, there is a unique subextension of $\overline{\mathbb{F}_p}$ consisting of p^n elements.

3.2 Properties of finite fields

Proof. So recall that we have seen that the map $F_{p^n} : x \mapsto x^{p^n}$ is a homomorphism. $\implies$ $\{x | F_{p^n}(x) = x\}$ is a subfield (it contains F_p, it contains the roots of $Q_n(x) = X^{p^n} - x$).

This subfield is exactly the splitting field of Q_n, and since Q_n does not have multiple roots (this can be seen by verifying that Q_n is relatively prime with its derivative $Q_n' = 1$) $\implies$ there are exactly p^n roots $\implies$ this is a splitting field of Q_n = the roots of Q_n = field of p^n elements.

Conversely, we show that any field of p^n elements is a splitting field of Q_n. Let $|K| = p^n$ and $\alpha \in K$ then $\alpha^{p^n-1} =$ (provided that $\alpha \neq 0$). Indeed, the multiplicative group of K has cardinality $|K^*| = p^n - 1$. α is a root of $x^{p^n} - x$ and 0 is also a root $\implies$ K consist of roots of Q_n. This also answers the question why there is a unique subextension of $\overline{F_p}$, which has p^n elements. This is just because these subextension consists exactly of the roots of Q_n. The unicity of the subextension (of the image of the embedding of K into $\overline{F_p}$) also follows. □

Theorem 3.2.1. $\mathbb{F}_{p^n} \supset \mathbb{F}_{p^d} \iff d|n$.

Proof. $\Rightarrow$ is the multiplicativity of degrees in towers. $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] \cdot [\mathbb{F}_{p^d} : \mathbb{F}_p]$, $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$.

$\Leftarrow$: Conversely, suppose that $d|n$, then if $x^{p^d} = x$, the same is true for $x^{p^n} = x$. $\implies \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. □

Theorem 3.2.2. $\mathbb{F}_{p^n}$ is a stem field and a splitting field of any irreducible polynomial $P \in \mathbb{F}_p[x]$ of degree n.

Proof. Indeed a stem field of P has degree n over $\mathbb{F}_p$. So this is F_{p^n}.

Let α be a root of P, $\alpha \in \mathbb{F}_{p^n}$, $\implies Q_n(\alpha) = 0$ (since Q_n has as roots exactly all elements of $\mathbb{F}_{p^n}$). $P|Q_n \implies P$ splits in $\mathbb{F}_{p^n}$. □

Corollary 3.2.3. $Q_n = \prod_{d|n} \prod_{P \text{ irred. monic and deg } P=d} P$.

Proof. We have already seen that all such P divide Q_n (since the stem field is $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$, so $Q_n(\alpha) = 0$ if α is a root). $\implies \prod_{d|n} \prod_{P:*(P,d)} P|Q_n$,with the condition $*(P,d) = P$ irreducible monic and deg $P = d$. Q_n has no multiple roots $\implies$ there are no multiple factors.

What remains to prove is that there are no other irreducible factors of Q_n. So let R be an irreducible factor of Q_n. Then if α is a root of R, $Q_n(\alpha) = 0$. So this means that $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n} \implies \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$, $d|n \implies$ deg $R|n$. That is there are no other irreducible factors. □

3.3 Multiplicative group and automorphism group of a finite field

The next theorem say that the multiplicative group of a finite field is cyclic.

Theorem 3.3.1. K field. G finite subgroup of K^* (multiplicative group of K), then G cyclic.

Proof. The idea is to compare G and the cyclic group of order N, $\mathbb{Z}/N\mathbb{Z}$, where $N = |G|$. Let $\psi(d)$ detote the number of elements of order d in G. We need to prove that $\psi(N) \neq 0$. We know that $N = \sum \psi(d)$. Let $\phi(d)$ detote the number of elements of order d in $\mathbb{Z}/N\mathbb{Z}$.

$\mathbb{Z}/N\mathbb{Z}$ contains a single cyclic subgroup of order d, $d|N$ (the subgroup generated by N/d). $\phi(d)$ = number of generators of $\mathbb{Z}/N\mathbb{Z}$ = number of numbers between 1 and $d-1$, which are prime to d. So $\phi(n) \neq 0$.

Claim: either $\psi(d) = 0$ or $\psi(d) = \phi(d)$. This is sufficient since the $\sum \psi(s) = \sum \psi(d)$. Proof of the claim. If there is no element of order d in G, then of course $\psi(d) = 0$. If $\exists x \in G$, x order $d \implies x$ is a root of the polynomial $x^d - 1$. The roots of such a polynomial form a cyclic subgroup of G. So G, as well as $\mathbb{Z}/N\mathbb{Z}$ has a single subgroup of order d (which is cyclic) or no such subgroup at all.

If $\phi(d) \neq 0 \implies$ there is such a subgroup. $\psi(d)$ = number of generators of that subgroup $= \phi(d)$.

In particular $\psi(d) \leq \phi(d)$, but in fact there must be equality, because $\sum_{d|N} \psi(d) = \sum_{d|N} \phi(d) \implies \psi(d) = \phi(d)$. In particular $\psi(n) \neq 0$. □

Corollary 3.3.2. Let $K \supset \mathbb{F}_p$, $[K : \mathbb{F}_p] = n \implies \exists \alpha$ such that $K = \mathbb{F}_p(\alpha)$. In particular $\exists$ an irreducible polynomial of degree n over $\mathbb{F}_p$.

Well, you might object and say this has already been shown. We have seen that $F_(p^N)$ is a stem field of any irreducible polynomial of degree N, but this corollary is actually stronger because when we've been discussing those stem fields we did not say that such polynomials existed.

Proof. It suffices to take α = generator of K^*. □

Corollary 3.3.3. The group of automorphisms of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is cyclic, generated by the Frobenius map, $F : x \mapsto x^p$.

Proof. $X^{p^n} = X \; \forall x \in \shortmid^{\ltimes}$ so $F^n = Id$.

On the other hand the order of Frobenius is exactly n, ord$(F) = n$: If $m < n$, then $F^m \neq Id$ (because $x^{p^m} - x = 0$ has only p^m roots and $p^m < p^n$).

Finally $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, where α is a root of irreducible polynomial of degree n, so it cannot have more than n automorphisms. This α goes to another root of P under an automorphism of $\mathbb{F}_{p^n}$. So the cardinality of this group is at most n, $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq n$ then it is n and the group is cyclic generated by F. □

3.4 Separable elements

Our next topic is separable extensions. We would like to say that a spliting polynomial spliting field of an irreducible polynomial has many automorphisms. So

E spliting field of an irreducible polynomial "has many automorphisms": if α, β roots of P, $E \supset K[\alpha]$, $E \supset K[\beta]$. $\exists$ isomorphism $\phi : K[alpha] \to K[beta]$ over K. By extension theorem, I can extend it to an automorphism of E.

There is one problem about this. Is it true, that an irreducible polynomial of degree n has many (n) roots? The answer is yes in characteristic 0. But not always if the characteristic of K is a prime number p. An irreducible polynomial in characteristic p can have multiple roots. This means that $\gcd(P, P') \neq 1$.

In characteristic 0 this cannot happen (deg $P <$ deg P' and $P' \neq 0$ when P is nonconstant $\implies$ P does not divide P').

In characteristic p, P' can vanish. And then GCD can be equal to the polynomial P. How can P' vanish? P' vanishes exactly when P is a polynomial in x^p. That is $P = \sum a_i x^i$, with $a_i \neq 0$ only if i is divisible by p. Take $r = \max h$ such that P is a polynomial in x^{p^h}, that is, $a_i = 0$ whenever p^h does not divide i. p^h does not divide i.

Proposition 3.4.1. $P(x) = Q(x^{p^r})$ and $Q' \neq 0$. In particular $(Q, Q') = 1$ and Q does not have multiple roots. In addition, all roots of P have multiplicity p^r.

Proof. If λ is a root of P, then $P = (x - \lambda) \cdot R$. Then $mu = \lambda^{p^r}$ is a root of Q. So $Q(y) = (y - lambda^{p^r}) \cdot S$, where λ is not a root of S. $\implies$ $P(x) = (x^{p^r} - \lambda^{p^r}) S(x^{p^r}) = (x - \lambda)^{p^r} S(x^{p^r})$ and λ is not a root of $S(x^{p^r})$. $\implies$ The multiplicity of λ is p^r. □

Definition Let $P \in K[x]$ be irreducible. Then it is called **separable** if it is prime to its derivative, $(P, P') = 1$ [so it does not have multiple roots]. The **separable degree** of P is the degree of Q is above, $d_{\text{sep}}(P) = \deg Q$. The **degree of inseparability** of P is the degree of P over the degree of Q, $d_i(P) = \frac{\deg P}{\deg Q} (= p^r)$. P is called **purely inseparable** if $\deg P = d_i(P)$ (then $P = x^{p^r} - a$).

Definition L algebraic extension of K. $\alpha \in L$ is called **separable** or **purely inseparable** over K if $P_{\min}(\alpha, K)$ has this property.

Proposition 3.4.2. If α is separable over K, then $|\mathrm{Hom}_K(K(\alpha), \overline{K})| = \deg P_{\min}(\alpha, K)$ (in general $|\mathrm{Hom}_K(K(\alpha), \overline{K})| = d_{\text{sep}} P_{\min}(\alpha, K)$).

Proof. The proof is obvious because the separable degree is just the number of distinct roots of this minimal polynomial. And we can send α into any of those roots. □

3.5 Separable degree, separable extensions

Let me generalize this property to the case of fields which are not necessarily given as $K(\alpha)$.

L finite extension of K.

Definition $[L : K]_{\text{sep}} = |\text{Hom}_K(L, \overline{K})|$. (Again, if $L = K(\alpha)$ then this degree is just the number of distinct roots of its minimal polynomial).

The extension L is separable over K if $[L : K]_{\text{sep}} = [L : K]$.

$[L : K]_i = \frac{[L:K]}{[L:K]_{\text{sep}}}$.

Theorem 3.5.1. 1. $K \subset L \subset M$ $[M : K]_{\text{sep}} = [M : L]_{\text{sep}} \cdot [L : K]_{\text{sep}}$ and M separable over $K \iff M$ separable over L and L separable over K.

2. TFAE:

   (a) L is separable over K

   (b) $\forall \alpha \in L$, α is separable over K

   (c) L is generated over K by a finite number of separable elements, $L = K(\alpha_1, \alpha_2, \cdots \alpha_n)$

   (d) $L = K(\alpha_1, \alpha_2, \cdots \alpha_n)$ and α_i separable over $K(\alpha_1, \alpha_2, \cdots \alpha_{i-1})$

Remark: the same holds when we replace separability by pure inseparability.

Proof. Part one. $\forall \phi : L \to \overline{K}$ extends to $\widetilde{\phi} : M \to \overline{K}$ (by the extension theorem). In fact, there are exactly $[M : L]_{\text{sep}}$ ways to do this. Since since given ϕ, one considers $\overline{K}$ as $\overline{L}$. (An algebraic closure of K is also an algebraic closure of L once an embedding of L into $\overline{K}$ is given.) Thus $[M : K]_{\text{sep}} = [M : L]_{\text{sep}} \cdot [L : K]_{\text{sep}}$.

Equivalence of separability: just the fact that the separable degree of an extension over K does not exceed the true degree, $[E : K]_{\text{sep}} \leq [E : K]$.

The last fact is proved by induction using the fact that this is true for $E = K(\alpha)$.

Part two. (a) $\implies$ (b). The first part implies that any subextension $K(\alpha)$ of a separable extension L is separable.

(b) $\implies$ (c). Obvious. If any element is separable then the generators are also separable.

(c) $\implies$ (d). This is clear because $P_{\min}(a_i, K(\alpha_1, \cdots \alpha_{i-1}))$ divides $P_{\min}(a_i, K)$. If $P_{\min}(a_i, K)$ ($\iff$ has distinct roots), so is its divisor $P_{\min}(a_i, K(\alpha_1, \cdots \alpha_{i-1}))$.

(d) $\implies$ (a). This can be proved by induction as above. □

One might ask, is the notion of separability defined for extensions which are not necessarily finite? Yes, in this case it is best to define a separable extension as such extension that all its elements are separable.

In particular, if L over K is not necessarily finite and algebraic extension, we can define L separable, the separable closure of K in L, as $L^{\text{sep}} = \{x | x \text{ separable over } K\}$. (A separable element is by definition algebraic, it has minimal polynomial). So the preceding theorem implies that this L^{sep} is a subfield, a subextension called **separable closure** of K in L. L is purely inseparable over L^{sep}.

Remark: if the char $K = 0$, then any extension is separable. And if char $K = p$, then a purely inseparable extension has degree p^r, and always this degree of inseparability is $[L : K]_i = p^r$.

3.6 Perfect fields

Let K be a field with char $K = p > 0$, p prime number.

Definition K is **perfect** if the Frobenius automorphism, $F : K \to K$, $x \mapsto x^p$, is surjective.

Example A finite field is always perfect. Since an injective self-map of a finite set is surjective.

Example An algebraically closed field is perfect. Since $x^p - a$ has a root α for any a, so in particular, $a = F(\alpha)$.

Example Take $K = \mathbb{F}_p(x)$ (this is a variable x) the field of rational functions in one variable $f(x)/g(x)$, where $f, g \in \mathbb{F}_p[x]$, over $\mathbb{F}_p$. Im $F = \mathbb{F}_p(x^p) \neq \mathbb{F}_p(x)$. $\implies$ K is not perfect.

Theorem 3.6.1. K is perfect iff all irreducible polynomials over K are separable $\iff$ all algebraic extensions of K are separable. (Separability only makes sense for algebraic extensions.)

Proof. $\Rightarrow$: Suppose K perfect. Let me take an irreducible polynomial $P \in K[x]$, suppose that P is a polynomial in some power of x, $P(x) = Q(x^{p^r}) = \sum a_i(x^{p^r})^i$. Since K perfect, we can extract p-th roots of a_i's and we can do it repeatedly. So $\exists b_i \in K$, such that $b^{p^r} = a_i$. So $P = (\sum b_i x^i)^{p^r}$ is not irreducible unless $r = 0$. If it's irreducible then it's separable.

$\Leftarrow$: If K is not perfect, then $\exists a \notin \text{Im } F$. Then $x^{p^r} - a$ is irreducible. In fact, all roots in $\overline{K}$ are the same x with $x^{p^r} = a$. And $x^{p^{r-1}} \notin K$. We have already seen that in this case the degree of $K(x)$ over K is exactly p^r, so this polynomial is irreducible. □

3.7 Summary

We have been considering $[L : K] < \infty$, a finite field extension, and we have defined separability. We have seen that, if L is generated over K by a finite number of separable elements, $\alpha_1, \cdots \alpha_r$, $\iff$ the number of $\text{Hom}_K(L, \overline{K}) = [L : K]$. (In general this number of homomorphisms is less or equal than the degree.)

These number of homomorphisms, we have called it "the separable degree" of L over K, $[L : K]_{\text{sep}}$. If L was generated by only one element α, $L = K(\alpha)$, this was clear since those homomorphisms were taking α to other roots of the minimal polynomial. And so, the number of homomorphisms was equal to the number of roots of the minimal polynomial. And in general, one can use induction and the multiplicativity over the degree (linear algebra) and the number of homomorphisms (extension theorem).

A separable extension was exactly an extension which had the right number of homomorphisms into the algebraic closure. In the future we will characterize separability in terms of tensor products.

Chapter 4

Tensor product. Structure of finite K-algebras

This will be a general digression which does not have much to do with field extensions.

4.1 Definition of tensor product

We consider a ring A and two A-modules, M and N. The tensor product M tensor N over A, $M \otimes_A N$, is another A-module together with an A-bilinear map $\phi : M \times N \to M \otimes_A N$ with the following universal property: if P is any A-module and $f : M \times N \to P$ A-bilinear (i.e. $\forall m$, $f_m : N \to P$,$n \mapsto f(m,n)$ and $\forall n$, $f_n : M \to P$,$m \mapsto f(m,n)$ are A-module homomorphisms (also A-linear homomorphisms of A-modules) then there exists a unique homomorphism of A-modules $\widetilde{f} : M \otimes_A N \to P$, such $f = \widetilde{f} \circ \phi$. This property characterizes $(\phi, M \otimes N)$ because if there is another pair $(\bar{\phi}, \overline{M \otimes N})$ with this property, then, by the very definition, we have mutually inverse homomorphisms of A-modules between our tensor products. The unity of such a thing follows directly from the definition.

Why does such a thing exist? One has to give a construction. The construction can be as follows: so, consider

$$\mathcal{E} = \{\text{maps } M \times N \to A, \text{ 0 almost everywhere}\}$$

(as sets, without any structure). What means almost everywhere? Outside of a finite set. For instance, we can take some kind of delta functions. $\delta_{m,n} : M \times N \to A$, $\delta_{m,n}(m,n) = 1$ and $\delta_{m,n}(m',n') = 0$, $\forall (m',n') \neq (m,n)$. Then $\mathcal{E}$ is a free A-module with base $\delta_{m,n}$. Now we have a map of sets $M \times N \to E$, $(m,n) \to \delta_{m,n}$. We can make it bilinear by changing $\mathcal{E}$. We can take a quotient. Take $\mathcal{F} \subset \mathcal{E}$ a submodule generated by $\delta_{m+m',n} - \delta_{m,n} - \delta_{m',n}$, $\delta_{m,n+n'} - \delta_{m,n} - \delta_{m,n'}$, $\delta_{am,n} - a\delta_{m,n}$, $\delta_{m,an} - a\delta_{m,n}$. Then the map $M \times N \to \mathcal{E}/\mathcal{F}$ is bilinear. And it is very easy to see that this has the desired universal property.

4.2 Tensor product of modules

If we have any bilinear map $f : M \times N \to P$, we can also define a map $\mathcal{E} \to P$, $\delta_{m,n} \to f(m,n)$. When the map f is bilinear, the map $\mathcal{E} \to P$ must factor through the quotient, $\mathcal{E}/\mathcal{F}$, as f is bilinear. This map must be zero on $\mathcal{F}$. So this factorization is determined by images of $\delta_{m,n}$. So this is unique. So we can call it ϕ $(M \times N \to \mathcal{E}/\mathcal{F})$ and we can identify $\mathcal{E}/\mathcal{F}$ (?) with $M \otimes N$.

$M \times N$ is generated by $m \otimes n$ ($\delta_{m,n}$'s mod F). In fact any element of my tensor product is a finite sum of such things. Remark: Not equal to $\{m \otimes n, m \in M, n \in N\}$, but $\forall x \in M \otimes N$, $x = \sum_{i=1}^{n} m_i \otimes n_i$.

Why haven't we just defined the tensor product by this construction? Why are we talking of this universal property? And the answer is because the advantage of the universal property is that the proofs become easy.

For example, if we have to prove commutativity, let us prove that $M \otimes_A N \cong N \otimes_A M$. Then it is very elegant with the universal property. Indeed $MtimesN \to N \otimes_A M$, $(m,n) \mapsto n \otimes m$ is bilinear. Therefore, it factors through the tensor product. We have $\alpha : M \otimes_A N \to N \otimes_A M$. In the same way obtain the inverse map of α, in the other direction.

In the same way we prove, for instance, that $A \otimes_A M \cong M$ (isomorphic).

More seriously: We have seen that, if M is generated by $e_1, \cdots e_n$, and N is generated by $\epsilon_1, \cdots \epsilon_m$, $\implies$ $M \otimes_A N$ is generated by $e_i \otimes \epsilon_j$. We can also prove:

Proposition 4.2.1. If $e_1, \cdots e_n$ bases of M and $\epsilon_1, \cdots \epsilon_m$ is a basis of M, and $\epsilon_1, \cdots \epsilon_n$ is a basis of N, then $e_i \otimes \epsilon_j$, where $1 \leq i \leq n$ and $1 \leq j \leq m$, is a basis of $M \otimes_A N$. And this is easily done with the universal property.

Proof. Let us define a bilinear map $f_{i_0,j_0} : M \times N \to A$, $(\sum a_i e_i, \sum b_j \epsilon_j) \mapsto a_{i_0}, b_{j_0}$ is bilinear. So it factors through the tensor product $\widetilde{f}_{i_0,j_0} : M \otimes N \to A$, $e_{i_0} \otimes \epsilon_{j_0} \mapsto 1$ and other $e_i \otimes \epsilon_j \mapsto 0$.

So if $\sum_{i,j} \alpha_{ij} e_i \otimes \epsilon_j = 0$, then applying this $\widetilde{f_{i_0,j_0}}$, we see that $\alpha_{i_0 j_0} = 0$. Doing this for all i_0, j_0, we conclude that all coefficients are 0. The tensor product of K-vector spaces with basis $e_1, \cdots e_n$ and $\epsilon_1, \cdots \epsilon_m$ is a K-vector space with basis the $e_i \otimes \epsilon_j$. This is how it is often defined. One just introduces formally such a base and builds a vector spaces on this. But it is much better to use this universal property. □

4.3 Base change

One also has other more or less elementary properties of the tensor products. For instance, associativity $(M_1 \otimes_A M_2) \otimes_A M_3 \cong M_1 \otimes_A (M_2 \otimes_A M_3)$. (The easiest way to prove this, is to introduce a triple tensor product $M_1 \otimes_A M_2 \otimes_A M_3$ as a universal object for trilinear maps and then show that both parts are isomorphic to this object).

Let me talk now about the base change. So, we have a ring A. Another ring B, which is an A-algebra. Also an extension of A as a ring. And let's have also M an A-module. And N and B-module. I can make N into A-module just forgetting the multiplication by the B-module structure.

You can make a B-module of M by considering $B \otimes_A M$. Indeed we can introduce the B-module structure on $B \otimes_A M$ by setting $b(b' \otimes m) = bb' \otimes m$.

Example *Complexification of a real vector space.* If you have a complex vector space $\mathbb{C}^n$, then you can make a real vector space $\mathbb{R}^{2n}$ of this just by forgetting the complex structure. If here you had basis $e_1, \cdots e_n$, then you just forget that you can multiply it by imaginary numbers and so, you obtain the basis $e_1, \cdots e_n, ie_1, \cdots ie_n$. But then you forget all together about this i and you redefine them as $v_1 = ie_1, \cdots v_n = ie_n$. Now, if you complexify, if you want to make a complex vector space out of $\mathbb{R}^{2n}$. Now, take $\mathbb{C} \otimes \mathbb{R}^{2n}$ with basis of $e_1, \cdots e_n, v_1, \cdots v_n$. (More precisely, one should write, $1 \otimes e_1, \cdots 1 \otimes v_n$. Of course, you can also go in the other way. $\mathbb{R}^n$ with basis $e_1, \cdots e_n$, then make it into a complex vector space by tensoring with $\mathbb{C}$: $\mathbb{C}^n = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n$. $\mathbb{C}$-basis $1 \otimes e_i$, and then you obtain $\mathbb{R}^{2n}$ (by forgetting the complex structure) with basis $1 \otimes e_i$ and $i \otimes e_i$.

In general, if M is a free A-module with base $e_1, \cdots e_n$ and we tensor it up with B, $B \otimes_A M$, this will be a free B-module with base $1 \otimes e_1, \cdots 1 \otimes e_n$. We also have a couple of important maps of A-modules: $M \to B \otimes_A M$, $m \mapsto 1 \otimes m$ and also we have a map in the other direction. $B \otimes_A N \to N$, $b \otimes n \mapsto b_n$.(Recall N is a B-module, but the map is of A-modules. Of B-modules too.)

The proof is the same as that of the previous proposition: We construct certain bilinear maps and say that those factor over the tensor product and this implies that certain families are linearly independent.

Now let me formulate a very important theorem. Notations are as before.

Theorem 4.3.1. Base change theorem.

$\mathrm{Hom}_A(M,N) \leftrightarrow \mathrm{Hom}_B(B\otimes_A M, N)$ (bijection, the corresponding groups of homomorphisms are isomorphic).

Proof. We have $M \xrightarrow{\alpha} B\otimes_A M \xrightarrow{f} N$,$f \mapsto f\cdot\alpha$. In one direction, $M \xrightarrow{g} N$, $B\otimes_A M \xrightarrow{\mathrm{id}\otimes g} B\otimes_A N \xrightarrow{\mu} B$ $(b\otimes n \to b_n)$. $g \mapsto \mu\cdot(\mathrm{id}\otimes g)$. And then we check that those maps are mutually inverse. □

4.4 Examples. Tensor product of algebras

So let me give you an example of such a base change which deserves the name of a proposition.

Proposition 4.4.1. $I \subset A$ ideal. The ring B, the A-algebra, will be $A/I\otimes_A M \cong M/IM$.

(The ring B, the A-algebra, will be A/I. And we are going to base change M to an A/I-module, then we affirm that this is just M/IM. So IM is a submodule of M. We take the quotient module, and we affirm this is the same as the base change of M to A/I.)

Proof. We can define in one direction the map $M \to A/I\otimes_A M$, $m \mapsto 1\otimes m$. (This is the previous map α). Then we remark that this sends IM to 0, because if we have $im \mapsto 1\otimes im$, where $i \in I$, everything is A-linear, so we can put i into the other side: $im \mapsto i\otimes m$. And $i\otimes m = 0\otimes m = 0$ because now we are in A/I. $\implies$ α induces a map $\bar{\alpha} : M/IM \to A/I\otimes_A M$.

Now in the other direction we apply the *Base change theorem.* Consider the projection $M \to M/IM$ (map of A-modules) gives $(B = A/I)$ $B\otimes_A M \to M/IM$ a map of B-modules. One checks again that this is the inverse of $\bar{\alpha}$. □

Example Let's take $\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/3\mathbb{Z}$. What do we obtain? We may consider it as a base change of $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$. So:

$$\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \Big/ (2)\cdot\mathbb{Z}/3\mathbb{Z}$$

But 2 is invertible modulo 3. Thus This is just -1 in fact. But $(2)\cdot\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$. (2) is not a proper ideal in $\mathbb{Z}/3\mathbb{Z}$, it's equal to the whole ring, so the quotient is 0.

Example Another obvious example. If we base change a polynomial ring, we obtain again a polynomial ring only over B. $B\otimes_A A[x] \cong B[x]$. This is a very interesting example, if I base change $B\otimes A[x]/(P)$ what do we obtain? We obtain $B[x]/(P)$, but in $B[x]$ (ideal generated by P in $B[x]$.)

Tensor product of A-algebras

Let fix two A-algebras B and C. $\alpha : A \to B$ and $\beta : A \to C$, which define the A-algebra structure on B and C, then we can introduce a new A-algebra $B \otimes_A C$. $B \otimes_A C$ is a ring with respect to the following operation $(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'$. In fact, this has the following universal property:

$$\begin{tikzcd}
& B \otimes_A C & \\
B \arrow[ur, "\phi"] & & C \arrow[ul, "\psi"'] \\
& A \arrow[ul, "\alpha"] \arrow[ur, "\beta"'] &
\end{tikzcd}$$

So $\phi : b \mapsto b \otimes 1$, $\psi : c \mapsto 1 \otimes c$. For any A-algebra D one has $\mathrm{Hom}_A(B \otimes_A C, D) \rightleftharpoons \mathrm{Hom}_A(B, D) \times \mathrm{Hom}_A(C, D)$ (bijection). If we have some homomorphism, say $h : B \otimes_A C \to D$, this is the same as giving two homomorphisms, let's say $f : B \to D$ and $g : C \to V$ such that all maps in this diagonal commute. (The diagram commutes.)

So if we have h we can define f and g: $h \mapsto (h \cdot \phi, h \cdot \psi)$ and conversely, given f and g, can define $h(b \otimes c) = f(b) \cdot g(c)$.

Okay, but I shall not say any more on this, this is just for the general culture. The main point for us is that the tensor product of the A-algebras is itself an A-algebra by this very simple rule, componentwise multiplication. Let us give an example.

Example Consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. How to describe the ring structure? What does it mean?

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes \mathbb{R}[x] \Big/ (x^2+1) \cong \mathbb{C}[x] \Big/ (x^2+1) \tag{4.1}$$

$$\cong \mathbb{C}[x] \Big/ (x+i) \times \mathbb{C}[x] \Big/ (x-i) \tag{4.2}$$

$$\cong \mathbb{C} \times \mathbb{C} \tag{4.3}$$

The next to last isomorphism is due to the Chinese remainder theorem.

This ring is not a field. $\mathbb{C}$ is a field but this tensor square has zero divisors, and so not a field. How to identify a zero divisor? The class of $\overline{x+i}$ is a zero divisor and is represented by $1 \otimes \overline{X} + i \otimes \bar{1}$ and in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ it is $1 \otimes i + i \otimes 1$.

4.5 Relatively prime ideals. Chinese remainder theorem

4.6 Structure of finite algebras over a field. Examples

Chapter 5

to do

5.1 to do

Chapter 6

to do

6.1 to do

Chapter 7

to do

7.1 to do

Chapter 8

to do

8.1 to do

Chapter 9

to do

9.1 to do