Galois Theory (all lectures)

Damian RÖSSLER*

March 15, 2021

PLEASE LET ME KNOW OF ANY MISTAKES OR TYPOS THAT YOU FIND IN THESE NOTES

Contents

1 Preamble **3**

2 Some basic commutative algebra **4**

2.1 Rings and domains 4

2.2 Fields 6

2.3 Rings of polynomials 6

2.4 Actions of groups on rings 9

3 Field extensions **12**

3.1 Definitions 12

3.2 Separability 13

3.3 Simple extensions 15

3.4 Splitting fields 16

3.5 Normal extensions 18

4 Galois extensions **21**

4.1 Overview 21

4.2 Artin's lemma 22

4.3 The fundamental theorem of Galois theory 24

4.4 The theorem of the primitive element 27

*Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom

5 Special classes of extensions **28**

5.1 Cyclotomic extensions 28

5.2 Kummer extensions 30

5.3 Radical extensions 32

5.3.1 Solvable groups 32

5.3.2 Solvability by radicals 34

5.3.3 The solution of the general cubical equation 38

6 Some group facts. Insolvable quintics. **40**

7 The fundamental theorem of algebra via Galois theory **42**

1 Preamble

The following notes are a companion to my lectures on Galois Theory in Michaelmas Term 2020 (at the University of Oxford). Galois theory was introduced by the French mathematician Évariste Galois (1811-1832). É. Galois wrote a memoir entitled "Théorie des équations" at the age of seventeen, which contains most of the theory that will be described in this course. Our presentation of the material will however differ from his in some respects. We follow the lead of the Austrian mathematician E. Artin (1898-1962), whose approach to Galois theory forms the basis of most modern courses and textbooks on the subject.

Some history. É. Galois sent his memoir to various famous mathematicians of his day (among them Cauchy and Poisson) but they showed little interest. He died in a duel at the age of twenty. A revised form of his memoir was found in his papers after his death. This revised form was published by Liouville in 1846.

A basic reference for this course is the book *Galois Theory* (Springer) by J. Rotman. Another excellent textbook on the topic is *Galois Theory* (Routledge, fourth edition) by I.-N. Stewart.

The reader might also want to consult E. Artin's lectures on Galois Theory, which are available here:

`https://projecteuclid.org/euclid.ndml/1175197041`

Caveat emptor. These notes are not very polished and they only give a bare outline of the theory (and they are probably not free of typos and small notational mistakes). For more details, consult the textbooks.

The basic idea of Galois Theory is the following.

Let $P(x) \in \mathbb{Q}[x]$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the roots of $P(x)$. Let $F := \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{C}$ be the smallest subfield of $\mathbb{C}$, which contains $\alpha_1, \ldots, \alpha_n$. Then we may consider the group

$$G := \{\text{field automorphisms of } F\}.$$

By construction, the elements of G permute the α_i, and if an element of G fixes all the roots, then it must be the identity (exercise - or see further below). Thus there is a natural injection $\iota : G \hookrightarrow S_n$, such that $\alpha_{\iota(g)(i)} = \alpha_{g(\alpha_i)}$, for $i \in \{1, \ldots, n\}$. In particular, G is finite.

One may thus associate a finite group with any polynomial with rational coefficients.

The fundamental insight of É. Galois was that the group theoretic properties of G provide crucial information on $P(x)$. For instance, he noticed that the structure of G alone determines whether it is possible to express the roots of $P(x)$ from its coefficients using a closed formula containing only polynomial expressions and extractions of k-th roots (for $k \geq 1$). A polynomial with the latter property is called solvable by radicals. Using his theory, Galois was then able to answer in the negative the following age-old question (which had been tackled unsuccessfully by several Renaissance mathematicians): are there polynomials, which are not solvable by radicals? Another question, which can be answered using Galois theory is the question of the existence of a ruler-compass construction, which trisects an arbitrary angle (an old problem in Euclidean geometry). Again, the answer is negative.

Galois Theory was vastly generalised in the 1950s and 1960s by A. Grothendieck, who saw it as a special case of what is now called *faithfully flat descent*.

Prerequisites of the course. We expect the reader to be familiar with the contents of the Part A course Rings and Modules. If he/she did not attend this course, we suggest studying the material of the Rings and Modules course alongside the material of the present course.

Basic notational conventions.

"A:=B" means "A is defined by B".

"wrog" means "without restriction of generality".

"st" is a shorthand for "such that".

"iff" means "if and only if".

$\#S$ is the cardinality (number of elements) of the set S.

"$A \Leftrightarrow B$" means "A is equivalent to B".

If G is a group and $H \subseteq G$ is a normal subgroup, we shall write G/H for the quotient group and $[\bullet]_H : G \to G/H$ for the quotient map (which is a map of groups).

"$S \hookrightarrow T$" an injective map from the set S to the set T.

2 Some basic commutative algebra

The material presented in this section was already covered in the Rings and Modules course.

2.1 Rings and domains

A (unitary) *ring* is a quadruple $(R, +, \cdot, 1, 0)$, where R is a set, 0 and 1 are elements of R, and $+$ and $\cdot$ are maps

$$+ : R \times R \to R \quad \text{(addition)}$$

and

$$\cdot : R \times R \to R \quad \text{(multiplication)}$$

st

- $(R, +, 0)$ is an abelian group;

- (associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$;

- (distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$;

- $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

A ring is *commutative*, if $a \cdot b = b \cdot a$ for all $a, b \in R$.

If $(R, +, \cdot, 1, 0)$ and $(S, +, \cdot, 1, 0)$ are rings, a *ring homomorphism (or ring map)* from $(R, +, \cdot, 1, 0)$ to $(S, +, \cdot, 1, 0)$ is a map $\phi : R \to S$, such that $\phi(1) = 1$ and for all $a, b \in R$,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

and

$$\phi(a + b) = \phi(a) + \phi(b).$$

There is an obvious notion of subring of a ring $(R, +, \cdot, 1, 0)$.

From now on, unless explicitly stated otherwise, all rings will be commutative. A ring will be a commutative ring from now on.

If $(R, +, \cdot, 1, 0)$ is a ring, we shall mostly use the shorthand R for $(R, +, \cdot, 1, 0)$. Also, if $r, t \in R$, we shall often write rt for $r \cdot t$. When we want to insist on the fact that 1 is an element of R, we shall write 1_R for 1. Similarly, when we want to insist on the fact that 0 is an element of R, we shall write 0_R for 0.

If $a \in R$ is an element of a ring, we shall write $a^{-1} \in R$ for the element st $a \cdot a^{-1} = 1$, *if it exists* (in which case it is unique). This element is called the *inverse* of a (if it exists). If a has inverse, then we say that a is *invertible*, or is a *unit*. We shall write R^* for the set of units in R. The set R^* is naturally a commutative group under multiplication.

A ring is *integral (or a domain, or an integral domain)* if, for any $a, b \in R$, the equation $a \cdot b = 0$ implies that either $a = 0$ or $b = 0$.

If R is a domain, an element $r \in R \backslash \{0\}$ is called *irreducible*, if whenever $r = r_1 r_2$, then either r_1 or r_2 is a unit.

Example. $\mathbb{Z}$ and $\mathbb{C}[x]$ are integral domains.

A subset $I \subseteq R$ of R is called an *ideal*, if it is an additive subgroup and for all $a \in R$ and $b \in I$, we have $a \cdot b \in I$.

If H is a subset of R, then set

$$(H) := \{\text{finite } R\text{-linear combinations of elements of } H\}$$

is an ideal (exercise), the *ideal generated by* H.

An ideal, which has the form (r) for some $r \in R$, is called *principal*.

If $r, t \in R$, the notation $r|t$ mean $t \in (r)$.

If $f : R \to S$ is a ring map, then the subset of R

$$\ker(f) := \{r \in R \,|\, f(r) = 0\}$$

is an ideal of R (exercise). This ideal is called the *kernel* of f.

Example. Any ideal of $\mathbb{Z}$ is principal (because $\mathbb{Z}$ is Euclidean - see below).

If $I \subseteq R$ is an ideal, the relation $\bullet \equiv \bullet \,(\text{mod } I)$ on R, st

$$a \equiv b \,(\text{mod } I) \text{ iff } a - b \in I$$

is an equivalence relation (verify). The set of equivalence classes of $\bullet \equiv \bullet (\text{mod } I)$ is denoted R/I. There is a natural map $[\bullet]_I : R \to R/I$ sending an element r to its equivalence class $[r]_I \in R/I$, and there is a unique ring structure on R/I, such that this map is a ring homomorphism. We shall always implicitly endow R/I with this ring structure.

If $f : R \to S$ is a ring map, then there a unique ring map $f' : R/\ker(f) \to S$, such that $f(r) = f'([r]_{\ker(f)})$ for all $r \in R$. Furthermore, f' is injective. This follows from the first isomorphism theorem.

An ideal I in a ring R is said to be *prime* if R/I is a domain. It is said to be *maximal* if R/I is a field.

For any ring R, there a unique ring map $\phi : \mathbb{Z} \to R$, st

$$\phi(n) = 1 + \cdots + 1 \,(n\text{-times})$$

(exercise). The *characteristic* $\text{char}(R)$ of R is the unique $r \geq 0$, such that $(r) = \ker(\phi)$. If R is a domain, then $\text{char}(R)$ is either 0 or a prime number (why?).

2.2 Fields

A ring R is a *field* if $(R\backslash\{0\}, \cdot, 1)$ is a commutative group and if $0 \neq 1$. Note that the ring R is a field iff $1 \neq 0$ and all the elements of $R\backslash\{0\}$ are invertible.

Proposition-Definition 2.1. *Let R be a domain. Then there is a field F and an injective ring map*

$$\phi : R \to F$$

st if

$$\phi_1 : R \to F_1$$

is a ring map into a field F_1, then there is a unique ring map $\lambda : F \to F_1$, st $\phi_1 = \lambda \circ \phi$. The field F is thus uniquely determined, up to unique isomorphism. It is called the field of fractions of F. One often writes $F := \mathrm{Frac}(R)$.

Proof. See Rings and Modules (or any number of references). □

Lemma 2.2. *(i) Let K be a field and let $I \subseteq K$ be an ideal. Then either $I = (0)$ or $I = K$.*

(ii) Let K, L be fields and let $\phi : K \to L$ be a ring map. Then ϕ is injective.

Proof. (i) If $I \neq (0)$, then let $k \in I\backslash\{0\}$. By definition, k^{-1} exists and since I is an ideal $k^{-1} \cdot k = 1 \in I$. But $K = (1) \subseteq I$ and thus $I = K$.

(ii) Consider $\ker(\phi)$. If $\ker(\phi) = K$ then $\phi(1) = 1 = 0$, which is a contradiction to the fact that L is a field. Thus $\ker(\phi) = (0)$ by (i). In particular, ϕ is injective by the first isomorphism theorem (see above). □

END OF LECTURE 1

2.3 Rings of polynomials

Let R be a ring. We shall write $R[x]$ for the ring of polynomials in the variable x and with coefficients in R (see Rings and Modules for the formal definition). If $r \geq 0$ is an integer, we define $K[x_1, \ldots, x_r] := K$ if $r = 0$ and

$$K[x_1, \ldots, x_r] := K[x_1][x_2] \ldots [x_r].$$

Let $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$, where $a_d \neq 0$. We shall say that $P(x)$ is *monic* if $a_d = 1$. The natural number $\deg(P) := d$ is called the *degree* of $P(x)$. An element $t \in R$ is a *root* of $P(x)$ if $a_d t^d + \cdots + a_1 t + a_0 = 0$. By convention, we set the degree of the 0 polynomial to be $-\infty$.

Lemma 2.3. *If R is a domain, then so is $R[x]$.*

Proof. Let $P(x), Q(x) \in R[x]$ and suppose that $P(x), Q(x) \neq 0$. Write

$$P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$$

and

$$Q(x) = b_l x^d + \cdots + b_1 x + b_0 \in R[x]$$

with $a_d, b_l \neq 0$. Then

$$P(x) \cdot Q(x) = (a_d \cdot b_l)x^{d+l} + \dots$$

and thus, if $P(x) \cdot Q(x) = 0$, then $a_d \cdot b_l = 0$ and thus either $a_d = 0$ or $b_l = 0$, a contradiction. □

Notation. If K is a field, then we shall write $K(x)$ for the field of fractions of $K[x]$. More generally, if $r \geq 0$ is an integer, we shall write $K(x_1, \dots, x_r)$ for the field of fractions of $K[x_1, \dots, x_d]$.

Proposition 2.4 (Euclidean division)**.** *Let K be a field. Let $f, g \in K[x]$ and suppose that $g \neq 0$. Then there are two polynomials $q, r \in K[x]$ st $f = gq + r$ and $\deg(r) < \deg(g)$. The polynomials q and r are uniquely determined by these properties.*

In particular, $K[x]$ is Euclidean (see Rings and Modules for this notion).

Proof. See Rings and Modules. □

Corollary 2.5. *$K[x]$ is a PID.*

Proof. See Rings and Modules. □

Recall that a Principal Ideal Domain (PID) is a domain, which has the property, that all its ideals are principal. Note that if K is a field and $I \subseteq K[x]$ is an ideal, then any polynomial in I, which has degree $\min\{\deg(f) \mid f \in I\}$, is a generator of I (use Euclidean division).

Note that if R is a domain and $r, r' \in R$, then $(r) = (r')$ iff $r = ur'$, where u is a unit (exercise). Applying this to $R = K[x]$, when K is a field, we see that if $f, g \in K[x]$ are two monic polynomials, then $(f) = (g)$ iff $f = g$. Using this remark and the remark above, we see that if $I \subseteq K[x]$ is an ideal, then there is a unique monic polynomial $P(x) \in I$, whose degree is $\min\{\deg(f) \mid f \in I\}$, and such that $(P(x)) = I$.

A Unique Factorisation Domain (UFD) is a domain R, which has the following property. For any $r \in R\backslash\{0\}$, there is a sequence $r_1, \dots, r_k \in R$ (for some $k \geq 1$), st

(1) all the r_i are irreducible;

(2) $(r) = (r_1 \cdots r_k)$;

(3) if $r'_1, \dots, r'_{k'}$ is another sequence with properties (1) and (2), then $k = k'$ and there is a permutation $\sigma \in S_n$ st $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \dots, k\}$.

Proposition 2.6. *Any PID is a UFD.*

Proof. See Rings and Modules. □

We conclude Corollary 2.5 and Proposition 2.6 and the above remarks that for any monic polynomial $f \in K[x]$, there is a sequence of irreducible monic polynomials $f_1, \dots, f_k$, st $f = f_1 \cdots f_k$. Moreover, this sequence is unique up to permutation.

If $P_1(x), \dots, P_k(x) \in K[x]$, we shall write $\gcd(P_1, \dots, P_k)$ for the unique monic generator of the ideal $(P_1(x), \dots, P_k(x))$ generated by $P_1(x), \dots, P_k(x)$. The symbol gcd stands for "greatest common divisor".

Lemma 2.7. *Suppose that R is a UFD. An element $f \in R\backslash\{0\}$ is irreducible iff (f) is a prime ideal.*

Proof. Suppose that f is irreducible. We want to show that (f) is a prime ideal. By definition of a prime ideal, we have to show that if $f|p_1p_2$, then either $f|p_1$ or $f|p_2$. Write $p_1 = u \cdot r_1 \cdots r_k$ (resp. $p_2 = u' \cdot r'_1 \cdots r'_{k'}$)

where u is a unit and the r_i are irreducible (resp. u' is a unit and the r'_i are irreducible). Then we have

$$p_1 p_2 = (uu') \cdot r_1 \cdots r_k \cdot r'_1 \cdots r'_{k'}$$

and thus, by unicity, $r_1 \cdots r_k \cdot r'_1 \cdots r'_{k'}$ is the decomposition of $p_1 p_2$ into irreducibles (up to permutation). By unicity again, $f \in \{r_1, \ldots, r_k, r'_1, \ldots, r'_{k'}\}$ and thus f divides either p_1 or p_2.

Now suppose that (f) is a prime ideal. Suppose for contradiction that f is not irreducible. Then $f = f_1 f_2$, where f_1 and f_2 are not units. Now since (f) is prime, either $f|f_1$ or $f|f_2$. Suppose wrog that $f|f_1$, or equivalently that $f_1 f_2 | f_1$. This contradicts the fact that f_1 is irreducible. □

Lemma 2.8. *Let R be a PID. Let $I \subseteq R$ be a prime ideal and suppose that $I \neq 0$. Then I is a maximal ideal.*

Proof. Suppose not. Then there is an element $r \in R$, such that $r \notin I$ and such that the ideal $([r]_I)$ generated by $[r]_I$ in R/I is not R/I (on in other words, $[r]_I$ is not a unit in R/I). Now note that we have $([r]_I) = [(r, I)]_I$. So we see that $(r, I) \neq R$ and that $(r, I) \supset I$ (strict inclusion). Let $g \in R$ be st $(g) = (r, I)$ and $h \in R \backslash \{0\}$ be st that $(h) = I$ (g and h exist because R is a PID). Then $g|h$ but $h \not| g$. This contradicts the fact that h is irreducible (the fact that h is irreducible follows from Proposition 2.6 and Lemma 2.7). □

Another immediate consequence of Euclidean division is the following.

Proposition 2.9. *Let K be a field and let $f \in K[x]$ and $a \in K$. Then*

(i) a is a root of f iff $(x - a)|f$;

(ii) there is a polynomial $g \in K[x]$, which has no roots, and a decomposition

$$f(x) = g(x) \prod_{i=1}^{k} (x - a_i)^{m_i}$$

where $k \geq 0$, $m_i \geq 1$ and $a_i \in K$.

Proof. Clear. □

We end this paragraph with three useful criteria for irreducibility. For the proofs, see Rings and Modules.

Proposition 2.10 (Eisenstein criterion)**.** *Let*

$$f = x^d + \sum_{i=0}^{d-1} a_i x^i \in \mathbb{Z}[x]$$

Let $p > 0$ be a prime number. Suppose that $p|a_i$ for all $i \in \{1, \ldots, d-1\}$ and that p^2 does not divide a_0. Then f is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$, by the Gauss lemma).

Lemma 2.11. *Let $f \in \mathbb{Z}[x]$. Suppose that f is monic. Let $p > 0$ be a prime number and suppose that $f \pmod p \in \mathbb{F}_p[x]$ is irreducible. Then f is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$, by the Gauss lemma below).*

Here $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is the field with p elements and the expression $f \pmod p$ refers to the polynomial in $\mathbb{F}_p[x]$, which is obtained by reducing all the coefficients of f modulo p.

Lemma 2.12 (Gauss lemma)**.** *Let $f \in \mathbb{Z}[x]$. Suppose that f is monic. Then f is irreducible in $\mathbb{Z}[x]$ iff f is irreducible in $\mathbb{Q}[x]$.*

The lemma of Gauss is proven using a special function, called the (Gauss) content function. To define it, we need an auxiliary function. Let p be a prime number. Let $r \in \mathbb{Q}^*$ be a rational number. Let $p_1 \dots, p_k$ be prime numbers. Suppose that $|r| = p_1^{m_1} \dots p_k^{m_k}$, where $m_i \in \mathbb{Z}$. We define

$$\mathrm{ord}_p(r) := m_i$$

if $p = p_i$ for some $i \in \{1, \dots, k\}$ and

$$\mathrm{ord}_p(r) = 0$$

if $p \neq p_i$ for all $i \in \{1, \dots, k\}$.

Let now

$$P(x) = c_d x^d + \dots + c_0 \in \mathbb{Q}[x] \backslash \{0\}.$$

Then the content $c(P)$ is defined as

$$c(P) := \prod_{p \text{ prime}} p^{\min\{\mathrm{ord}_p(c_i) \,|\, i \in \{0,\dots,d\}\}}$$

Clearly, we have $c(P) \in \mathbb{Z}$ iff $P(x) \in \mathbb{Z}[x]$.

Lemma 2.13 (Gauss)**.** *If $P(x), Q(x) \in \mathbb{Q}[x] \backslash \{0\}$. Then $c(P \cdot Q) = c(P)c(Q)$.*

Proof. See Rings and Modules. □

We also refer to the Rings and Modules course for the proof of Lemma 2.12 (which, as explained above, uses Lemma 2.13).

2.4 Actions of groups on rings

Let S be a set and let G be a group. Write $\mathrm{Aut}_{\mathrm{Sets}}(S)$ for the group of bijective maps $a : S \to S$ (where the group law is given by the composition of maps). An *action* of G on S is a group homomorphism

$$\phi : G \to \mathrm{Aut}_{\mathrm{Sets}}(S)$$

Notation. If $\gamma \in G$ and $s \in S$, we write

$$\gamma(s) := \phi(\gamma)(s).$$

We also sometimes write γs for $\gamma(s)$. We write S^G for the set of invariants of S under the action of G, ie

$$S^G := \{s \in S \,|\, \gamma(s) = s \ \forall \gamma \in G\}.$$

If $s \in S$, we let

$$\mathrm{Orb}(G, s) := \{\gamma(s) \,|\, \gamma \in G\}$$

be the *orbit* of s under G and

$$\mathrm{Stab}(G, s) := \{\gamma \in G \,|\, \gamma(s) = s\}$$

be the *stabiliser* of s (which is a subgroup of G).

We shall sometimes write $\mathrm{Orb}(r)$ in place of $\mathrm{Orb}(G, r)$ (resp. $\mathrm{Stab}(r)$ in place of $\mathrm{Stab}(G, r)$) when the underlying group G is clear from the context.

Now suppose that $S = R$, where R is a ring. We shall say that the action of G on R is *compatible with the ring structure of* R, or that G *acts on the ring* R, if the image of ϕ lies in the subgroup

$$\mathrm{Aut}_{\mathrm{Rings}}(R) \subseteq \mathrm{Aut}_{\mathrm{Sets}}(R)$$

of $\mathrm{Aut}_{\mathrm{Sets}}(R)$. Here $\mathrm{Aut}_{\mathrm{Rings}}(R)$ is the group of bijective maps $R \to R$, which respect the ring structure.

Lemma 2.14. *Let G act on the ring R.*

(i) R^G is a subring of R.

(ii) If R is a field, then R^G is a field.

Proof. (i) Clearly $\gamma(1) = 1$ for all $\gamma \in G$. Also, if $\gamma(a) = a$ and $\gamma(b) = b$ for some $\gamma \in G$, then $\gamma(ab) = \gamma(a)\gamma(b) = ab$ and $\gamma(a + b) = \gamma(a) + \gamma(b) = a + b$. This proves (i).

(ii) Suppose that $a \neq 0$ and that $\gamma(a) = a$ for some $\gamma \in G$. Then $\gamma(aa^{-1}) = \gamma(a)\gamma(a^{-1}) = \gamma(1) = 1 = a\gamma(a^{-1})$. Thus $\gamma(a^{-1})$ is an inverse of a and must thus coincide with a^{-1}. Since γ was arbitrary, any element of $R^G \backslash \{0\}$ has an inverse, and R^G is thus a field. $\square$

Let R be a ring and let $n \geq 1$. There is a natural action of S_n on the ring $R[x_1, \ldots, x_n]$, given by the formula

$$\sigma(P(x_1, \ldots, x_n)) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Definition 2.15. *A symmetric polynomial with coefficients in R is an element of $R[x_1, \ldots, x_n]^{S_n}$.*

Examples. For any $k \in \{1, \ldots, n\}$, the polynomial

$$s_k := \sum_{i_1 < i_2 < \cdots < i_k} \prod_{j=1}^{k} x_{i_j} \in \mathbb{Z}[x_1, \ldots, x_n]$$

is symmetric. It is called the k-th *elementary symmetric function* (in n variables). For instance, we have

$$s_1 = x_1 + \cdots + x_n$$

and

$$s_n = x_1 \cdots x_n.$$

The polynomials s_k appear in the following way in the context of polynomials in one variable. One computes that

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) = x^d - s_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + s_2(\alpha_1, \ldots, \alpha_d)x^{d-2} + - \cdots + (-1)^d s_d(\alpha_1, \ldots, \alpha_d)$$

In words: the coefficients of a polynomial are (up to sign) the symmetric functions of its roots.

Theorem 2.16 (Fundamental theorem of the theory of symmetric functions)**.**

$$R[x_1, \ldots, x_n]^{S_n} = R[s_1, \ldots, s_n].$$

Here is a more precise formulation. Let $\phi : R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ be the map of rings, which sends x_k to s_k and which sends constant polynomials to themselves. Then

(i) the ring $R[x_1, \ldots, x_n]^{S_n}$ is the image of ϕ;

(ii) ϕ is injective.

Proof. We shall sketch the proof of (i). We first introduce the lexicographic ordering on monomials. We shall write

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \overset{\text{DEF}}{\leq} x_1^{\beta_1} \cdots x_n^{\beta_n}$$

if either

- $\alpha_1 < \beta_1$

or

- $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdots x_n^{\alpha_n} \leq x_2^{\beta_2} \cdots x_n^{\beta_n}$.

The lexicographic ordering is similar to the alphabetic ordering on words.

Now let f be a symmetric polynomial. Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest monomial in f, for the lexicographic ordering. We must have $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.

To see this, note that, by definition, for any $\sigma \in S_n$, the monomial $x_1^{\alpha_{\sigma(1)}} \cdots x_n^{\alpha_{\sigma(n)}}$ must also appear in f. Now suppose for contradiction that $\alpha_1 < \alpha_2$. Apply to $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ the transposition σ, which swaps 1 and 2. We obtain the monomial $x_1^{\alpha_2} x_2^{\alpha_1} \cdots x_n^{\alpha_n}$. By the above, this polynomial also appears in f and by definition

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\alpha_2} x_2^{\alpha_1} \cdots x_n^{\alpha_n},$$

which is a contradiction. Hence $\alpha_1 \geq \alpha_2$. Now repeat this reasoning for α_2 and α_3, α_3 and α_4, etc.

Now one may compute that the largest monomial in the polynomial

$$s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$$

is also $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Thus we see that for some $c \in R$, all the monomials in the polynomial

$$f - c \cdot s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$$

are strictly smaller than $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for the lexicographic ordering. We now repeat all the above reasoning, with $f - c \cdot s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$ in place of f. We end up exhausting all the monomials in f and we obtain an expression for f as a polynomial in the s_i. $\square$

Example. $\sum_{i=1}^n x_i^2 = s_1^2 - 2s_2$.

Proposition-Definition 2.17.

(i) $\Delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$;

(ii) $\delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]^{A_n}$;

(iii) If $\sigma \in S_n$, *then* $\delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \text{sign}(\sigma) \cdot \delta(x_1, \ldots, x_n)$.

Here $\text{sign} : S_n \to \{-1, 1\} \subseteq \mathbb{Z}$ gives the *sign* of a permutation. It is a group homomorphism if $\{-1, 1\}$ is given its multiplicative group structure (see any first course on group theory for this). Here $A_n := \ker(\text{sign})$ is called the *alternating group*. The polynomial $\Delta(x_1, \ldots, x_n)$ is called the *discriminant*.

Proof. Exercise. Note that (ii) follows from (iii) and use the fact that any element of S_n is a product of transpositions. □

END OF LECTURE 2

3 Field extensions

3.1 Definitions

Let K be a field. A *field extension* of K, or K-extension, is an injection

$$K \hookrightarrow M$$

of fields. This injection endows M with the structure of a K-vector space.

Alternate notation: $M - K$, $M|K$, $M : K$. We shall mostly use the notation $M|K$.

A map from the K-extension $M|K$ to the K-extension $M'|K$ is a ring map $M \to M'$ (which is necessarily injective), which is compatible with the injections $K \hookrightarrow M$ and $K \hookrightarrow M'$.

If $M|K$ is a field extension, we shall write $\mathrm{Aut}_K(M)$ for the group of bijective maps of K-extensions from M to M (where the group law is the composition of maps). In other words, the group $\mathrm{Aut}_K(M)$ is the subgroup of $\mathrm{Aut}_{\mathrm{Rings}}(M)$, consisting of ring automorphisms, which are compatible with the K-extension structure of M.

Note that in fact any map of K-extensions from M to M is a bijection (use rank nullity), so that the assumption of bijectivity was redundant in the definition of $\mathrm{Aut}_K(M)$.

We say that the field extension is *finite* if $\dim_K(M) < \infty$.

We shall write $[M : K]$ for $\dim_K(M)$. The integer $[M : K]$ is called the *degree* of the extension $M|K$.

Proposition 3.1 (tower law)**.** *If $L|M$ and $M|K$ are finite field extensions, then we have*

$$[M : K] \cdot [L : M] = [L : K].$$

More precisely, if $m_1, \ldots, m_s$ is a basis of M as a K-vector space and $l_1, \ldots, l_t$ is a basis of L as a M-vector space, then the set $\{m_i l_j\}_{i \in \{1,\ldots s\}, j \in \{1,\ldots,t\}}$ is a basis for L as a K-vector space.

Proof. See Rings and Modules. □

Let $M|K$ be a field extension and let $a \in M$. We define

$$\mathrm{Ann}(a) := \{P(x) \in K[x] \,|\, P(a) = 0\}$$

The set $\mathrm{Ann}(a) \subseteq K[x]$ is called the *annihilator* of x. It is an ideal of $K[x]$ (easy).

We say that a is *transcendental* over K if $\mathrm{Ann}(a) = (0)$.

We say that a is *algebraic* over K if $\mathrm{Ann}(a) \neq (0)$.

If a is algebraic over K, then the *minimal polynomial* m_a is by definition the unique monic polynomial, which generates $\mathrm{Ann}(a)$ (see subsection 2.3). By definition, this polynomial has the property that it divides any polynomial with coefficients in K, which annuls (one also says annihilates) a.

Note. The ideal $\mathrm{Ann}(a)$ is prime, since there is an injection $K[x]/\mathrm{Ann}(a) \hookrightarrow M$ and M is a domain (see end of subsection 2.1). Now suppose that a is algebraic over K. Then, by Lemma 2.7, m_a is irreducible. This implies that a monic irreducible polynomial $P(x)$, which annihilates a, must be the minimal polynomial of a. Note also that $\mathrm{Ann}(a)$ is a maximal ideal by Lemma 2.8.

We say that a field extension $M|K$ is *algebraic* if for all $m \in M$, the element m is algebraic over K.

We say that a field extension $M|K$ is *transcendental* if it is not algebraic over K.

Lemma 3.2. *If $M|K$ is finite, then $M|K$ is algebraic.*

Proof. Let $m \in M$. Suppose that m is transcendental over K. Then there is an injection of K-vector spaces $K[x] \hookrightarrow M$. Since $K[x]$ is infinite dimensional, this contradicts the tower law. $\square$

3.2 Separability

Let K be a field. Let $P(x) \in K[x]$. Suppose that

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0.$$

We define

$$P'(x) = \frac{\mathrm{d}}{\mathrm{d}x}P(x) := da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1.$$

Here $d-i$ is understood as $1_K + \cdots + 1_K$ ($(d-i)$-times). The operation $P(x) \mapsto P'(x)$ is a formal analogue of the operation of derivation familiar from analysis. It satisfies similar formal rules. It is a K-linear map from $K[x]$ to $K[x]$ and it satisfies the "Leibniz rule":

$$\frac{\mathrm{d}}{\mathrm{d}x}(P(x)Q(x)) = \frac{\mathrm{d}}{\mathrm{d}x}(P(x))Q(x) + P(x)\frac{\mathrm{d}}{\mathrm{d}x}Q(x)$$

(see exercises).

We say that $P(x)$ *has no multiple roots* if $(P(x), P'(x)) = (1)$. Otherwise, we say that $P(x)$ *has multiple roots*. Equivalently, $P(x)$ has multiple roots iff $\gcd(P(x), P'(x)) \neq 1$.

Note the following fact, which justifies the terminology. If

$$P(x) = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_d)$$

then $P(x)$ has multiple roots iff there are $i, j \in \{1, \ldots, d\}$ such that $i \neq j$ and $\rho_i = \rho_j$. See the exercises for this (use the Leibniz rule).

Lemma 3.3. *Let $L|K$ be a field extension. Let $P(x), Q(x) \in K[x]$. Write $\gcd_L(P(x), Q(x))$ for the greatest common divisor of $P(x)$ and $Q(x)$ viewed as polynomials with coefficients in L. Then*

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x)).$$

Proof. This follows from the fact that a generator of $(P(x), Q(x))$ can be computed using Euclidean division. First view $P(x)$ as having coefficients in K. Suppose wrog that $\deg(Q) \leq \deg(P)$. Apply Euclidean division and write

$$P = Q_1 Q + R_1$$

We then have $(P,Q) = (Q,R_1)$. Note that $\deg(R_1) < \deg(Q) \leq \deg(P)$. Now apply Euclidean division again and write

$$Q = Q_2R_1 + R_2$$

$$R_1 = Q_3R_2 + R_3$$

$$R_2 = Q_4R_3 + R_4$$

$$\text{etc.}$$

We have $(Q,R_1) = (R_1,R_2) = (R_2,R_3) = \dots$ and $\deg(Q) > \deg(R_1) > \deg(R_2) > \deg(R_3) > \dots$ Since the sequence of the $\deg(R_i)$ is strictly decreasing, there must be a $k \geq 1$ st $\deg(R_k) = -\infty$, ie st $R_k = 0$. But then we have $(P,Q) = (R_{k-1},R_k) = (R_{k-1})$. In other words, R_{k-1} is a generator of (P,Q). Thus the polynomial $\gcd(P(x),Q(x))$ is the polynomial R_{k-1} divided by its highest non zero coefficient. Now, by the unicity statement in Euclidean division (see Proposition 2.4), if we view $P(x)$ and $Q(x)$ as polynomials with coefficients in L and apply the same procedure, we will obtain the same sequence of R_i. We conclude that $\gcd(P(x),Q(x)) = \gcd_L(P(x),Q(x))$. $\square$

Note. The algorithm described in the last lemma (to compute a generator of (P,Q)) is called the *Euclidean algorithm.*

Corollary 3.4 (of Lemma 3.3)**.** *Let K be a field and let $P(x) \in K[x]$. Let $L|K$ be a a field extension. Then $P(x)$ has multiple roots as a polynomial with coefficients in K iff it has multiple roots as a polynomial with coefficients in L. In particular, if $P(x) = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_d)$ in $L[x]$, then $P(x)$ has multiple roots as a polynomial with coefficients in K iff there are $i,j \in \{1,\dots,d\}$ such that $i \neq j$ and $\rho_i = \rho_j$.*

Proof. Clear. $\square$

Lemma 3.5. *Let $P(x),Q(x) \in K[x]$ and suppose that $Q(x)|P(x)$. Suppose that $P(x)$ has no multiple roots. Then $Q(x)$ has no multiple roots.*

Proof. Let $T(x) \in K[x]$ be st $Q(x)T(x) = P(x)$. Then by the Leibniz rule, we have

$$(P,P') = (Q'T + QT', QT) = (1)$$

If now Q and Q' were both divisible by a polynomial $W(x)$ with positive degree, then so would be $Q'T+QT'$ and QT. Then 1 would be divisible by $W(x)$, which is a contradiction. $\square$

Lemma 3.6. *Suppose that K is a field and that $P(x) \in K[x]\backslash\{0\}$. Suppose that* $\text{char}(K)$ *does not divide* $\deg(P)$ *and that $P(x)$ is irreducible. Then $(P,P') = (1)$.*

Proof. Let

$$P(x) = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. By definition, we have

$$P'(x) = da_dx^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1.$$

By assumption, we have $(d, \text{char}(K)) = (1)$ and so we see that $d \neq 0_K$ in K (see the definition of the characteristic of a ring). Thus $P'(x) \neq 0$. Now, since P is irreducible, any common divisor of P and P'

must be either a non zero constant, or P times a non zero constant. It cannot be equal to P times a non zero constant, because $\deg(P') < \deg(P)$. Hence it must be a non zero constant. In particular, $(P, P') = (1)$. $\square$

Let K be a field. We shall say that $P(x) \in K[x]\backslash\{0\}$ is *separable* if all the irreducible factors of $P(x)$ have no multiple roots. We deduce from Lemma 3.5 and Corollary 3.4 that this notion is invariant under field extension. Note that according to Lemma 3.6, an irreducible polynomial with coefficients in K, whose degree is prime to the characteristic of K, is separable. In particular, if $\mathrm{char}(K) = 0$, then any irreducible polynomial with coefficients in K is separable.

Definition 3.7. *Let $L|K$ be an algebraic field extension. We say that $L|K$ is separable if the minimal polynomial over K of any element of L is separable.*

Note that if K is a field and $\mathrm{char}(K) = 0$, then all the algebraic extensions of K are separable. This follows from the last remark.

Lemma 3.8. *Let $M|L$ and $L|K$ be algebraic field extensions. Suppose $M|K$ is separable. Then $M|L$ and $L|K$ are both separable.*

Proof. Clearly $L|K$ is separable. So let $m \in M$ and let $P(x) \in K[x]$ be its minimal polynomial over K. Let $Q(x)$ be the minimal polynomial of m over L. By assumption $Q(x)|P(x)$. Furthermore, again by assumption, $P(x)$ has no multiple roots over K. By Corollary 3.4, $P(x)$ also has no multiple roots over L. Finally, by Lemma 3.5, $Q(x)$ also has no multiple roots over L, so it is separable. Since $m \in M$ was arbitrary, $M|L$ is separable. $\square$

Example of a finite extension, which is not separable. Let $K := \mathbb{F}_2(t)$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ is the field with two elements. Let $P(x) := x^2 - t$. Since $P(x)$ is of degree 2 and has no roots in K (show this), it is irreducible. Let $L := K[x]/(P(x))$. Since $P(x)$ is irreducible, L is a field by Lemma 2.7 and Lemma 2.8. On the other hand, $P'(x) = 0$ so $(P', P) = (P) \neq (1)$. Now $P(x)$ is the minimal polynomial of $x \pmod{P(x)} \in K[x]/(P(x)) = L$. Hence the extension $L|K$ is not separable.

END OF LECTURE 3

3.3 Simple extensions

Let $\iota : K \hookrightarrow M$ be a field extension and let $S \subseteq M$ be a subset.

We define

$$K(S) := \bigcap_{L \text{ a field}, L \subseteq M,\, L \supseteq S,\, L \supseteq \iota(K)} L$$

This a subfield of M, the *field generated by S over K* and the elements of S are called *generators* of $K(S)$ over K. The field extension $M|K$ is the composition of the natural field extensions $K(S)|K$ and $M|K(S)$.

Note the following elementary fact. If $S = \{s_1, \ldots, s_k\}$, then

$$K(S) = K(s_1)(s_2)\ldots(s_k)$$

We say that $M|K$ is a *simple extension* if there is $m \in M$, such that $M = K(m)$.

Examples.

- Let $K = \mathbb{Q}$ and let $M = \mathbb{Q}(i, \sqrt{2})$ be the field generated by i and $\sqrt{2}$ in $\mathbb{C}$. Then M is a simple algebraic extension of $K = \mathbb{Q}$, generated by $i + \sqrt{2}$.

- Let $M = \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$ and let $K = \mathbb{Q}$. Then M is a simple transcendental extension of K, generated by x (note that x is transcendental over $\mathbb{Q}$).

Proposition 3.9. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Then there is a natural isomorphism of K-extensions*

$$K[x]/(P(x)) \simeq M$$

sending x to α.

Proof. The existence of the map follows from the definitions (see the end of subsection 2.1). Since $P(x) \neq 0$ (recall that α is algebraic over K), we deduce from Lemma 2.8 that $(P(x))$ is a maximal ideal. Thus the image of $K[x]/(P(x))$ in M is a field. By the definition of M, this field must be all of M. $\square$

Note. Under the assumptions of the proposition, this shows in particular that $[M : K] = \deg(P)$. Indeed, in the K-vector space $K[x]/(P(x))$, the set

$$1 \,(\mathrm{mod}\ \ (P(x))), x \,(\mathrm{mod}\ \ (P(x))), x^2 \,(\mathrm{mod}\ \ (P(x))), \ldots, x^{\deg(P)-1} \,(\mathrm{mod}\ \ (P(x)))$$

is a basis.

Corollary 3.10. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Let $K \hookrightarrow L$ be an extension of fields. Let $P(x)$ be the minimal polynomial of α over K. Then the maps of K-extensions $M \hookrightarrow L$ are in $1-1$-correspondence with the roots of $P(x)$ in L.*

Proof. Clear. $\square$

Note. It follows from Proposition 3.9 that a finitely generated algebraic extension is a finite extension.

Example. Let $M := \mathbb{Q}(i) \subseteq \mathbb{C}$ and let $K = \mathbb{Q}$. Let $L := \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. Then there is no map of K-extensions $M \hookrightarrow L$, because the roots of $x^2 + 1$ (which is the minimal polynomial of i over $\mathbb{Q}$) are $\pm i$, which do not lie in $L \subseteq \mathbb{R}$.

If $L = \mathbb{C}$, and M and K are as above, then there are two maps of K-extensions $M \hookrightarrow L$, which correspond to the two roots of $x^2 + 1$ in $\mathbb{C}$.

3.4 Splitting fields

Let K be a field.

Definition 3.11. *Let $P(x) \in K[x]$. We say that $P(x)$ splits in K, if for some $c \in K$, and some sequence $\{a_i \in K\}_{i \in \{1,\ldots,k\}}$, we have $P(x) = c \cdot \prod_{i=1}^{k}(x - a_i)$*

Example. $x^2 + 1 = (x - i)(x + i)$ splits in $\mathbb{C}$ but (famously!) not in $\mathbb{R}$.

A field L is *algebraically closed* if any polynomial with coefficients in L splits in L.

Note. If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$ then $P(x)$ has no roots in K (see Proposition 2.9), and in particular it does not split in K.

Definition 3.12. *A field extension $M|K$ is a splitting extension (or, less precisely, a splitting field) for $P \in K[x]$, if*

(i) $P(x)$ splits in M;

(ii) M is generated over K by the roots of $P(x)$ in M.

Theorem 3.13. *Let $P(x) \in K[x]$. Then*

(i) There exists a field extension $M|K$, which is a splitting extension for $P(x)$.

(ii) If $L|K$ is a splitting extension for $P(x)$, then L and M are isomorphic as K-extensions.

(iii) Let $L|K$ be a splitting extension for $P(x)$ and let $J|K$ be any K-extension. Then the images of all the maps of K-extensions $L \hookrightarrow J$ coincide.

Note that the isomorphism announced in (ii) is not canonical.

Proof.

(i) By induction on $\deg(P)$. If $\deg(P) = 1$, then $K|K$ is a splitting extension for $P(x)$. Suppose that $\deg(P) > 1$ and that the theorem is verified for any polynomial of degree $< \deg(P)$ (over any field). Let P_1 be an irreducible factor of $P(x)$. Let $M_1 := K[x]/(P_1(x))$. Then M_1 is a field by Lemma 2.7 and Lemma 2.8 and there is a natural map of rings $K \hookrightarrow M_1$, making it into a field extension. By definition, $P(x)$ has a root a in M_1 (corresponding to x in the presentation $M_1 = K[x]/(P_1(x))$). Now let M be a splitting field for $P(x)/(x-a) \in M_1[x]$ over M_1 (this exists by the inductive hypothesis). By construction, $P(x)$ splits in M. Let $a_2 \ldots, a_k$ be the roots of $P(x)/(x-a)$ in M. Then by the beginning of subsection 3.3 and Proposition 3.9, we have $M = K(a)(a_2)\ldots(a_k) = K(a, a_2, \ldots, a_k)$ and thus M is generated over K by its roots in M. Thus M is a splitting field of $P(x)$ over K.

(ii) By induction on $\deg(P)$. If $\deg(P) = 1$ then there is nothing to prove. Suppose that $\deg(P) > 1$. Let $a \in M$ be a root of $P(x)$ in M and let $Q(x) \in K[x]$ be its minimal polynomial. Then $Q(x)$ splits in M and also in L (since it divides $P(x)$). Let a_1 be a root of $Q(x)$ in L. Notice that $M|K(a)$ is a splitting extension of $P(x)/(x-a) \in K(a)$. Similarly $L|K(a_1)$ is a splitting extension of $P(x)/(x-a_1) \in K(a_1)$. Now let $J := K[x]/(Q(x))$. The ring J is a field, since $Q(x)$ is irreducible and furthermore there are natural isomorphisms $J \simeq K(a)$ and $J \simeq K(a_1)$ of K-extensions (by Proposition 3.9). Consider the J-extensions $M|J$ and $L|J$ arising from these isomorphisms. By the inductive hypothesis, these two J-extensions are isomorphic (since $\deg(P(x)/(x-a)) = \deg(P(x)/(x-a_1)) < \deg(P)$). By construction an isomorphism $M \simeq L$ of J-extensions is also an isomorphism of K-extensions, so we are done.

(iii) If there are no maps of K-extensions from L to J then the statement is empty. So suppose that there is a map $\phi : L \hookrightarrow J$ of K-extensions. Since L is generated over K by the roots of $P(x)$, the image of ϕ is generated over K by the images of these roots in J under ϕ. But these images are the roots of $P(x)$ in J.

To see this, let $\alpha_1, \ldots, \alpha_d$ be the roots of $P(x)$ in L, with multiplicities. Then we have

$$P(x) = x^d - \sigma_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \sigma_2(\alpha_1, \ldots, \alpha_d)x^{d-2} + - \cdots + (-1)^d \sigma_d(\alpha_1, \ldots, \alpha_d)$$

Thus the elements $\phi(\alpha_1), \ldots, \phi(\alpha_d)$ are the roots of

$$\begin{aligned} &x^d - \sigma_1(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{d-1} + \sigma_2(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{d-2} + - \cdots + (-1)^d \sigma_d(\phi(\alpha_1), \ldots, \phi(\alpha_d)) \\ &= x^d - \phi(\sigma_1(\alpha_1, \ldots, \alpha_d))x^{d-1} + \phi(\sigma_2(\alpha_1, \ldots, \alpha_d))x^{d-2} + - \cdots + (-1)^d \phi(\sigma_d(\alpha_1, \ldots, \alpha_d)) = P(x) \end{aligned}$$

(since the coefficients of $P(x)$ lie in K).

Now the set of roots of $P(x)$ in J does not depend on ϕ, hence the assertion. $\square$

Note the following useful fact. Let K be a field and let $P(x) \in K[x]$. Suppose that there is a field extension $K \hookrightarrow L$, where L is algebraically closed. Let $S \subseteq L$ be the roots of $P(x)$ in L. Then $K(S) \subseteq L$ is a splitting field for $P(x)$. This simply follows from the fact that $P(x)$ splits in $K(S)$ (since L is algebraically closed) and from the fact that $K(S)$ is generated by the roots of of $P(x)$ in $K(S)$ (by definition). This remark is often applied to $K = \mathbb{Q}$ and $L = \mathbb{C}$.

It can proven that for any field K, there is an algebraic field extension $K \hookrightarrow \bar{K}$, where $\bar{K}$ is algebraically closed. The extension $K \hookrightarrow \bar{K}$ is unique up to (non canonical) isomorphism and is called the *algebraic closure* of K. We shall not use this fact however.

END OF LECTURE 4

3.5 Normal extensions

Definition 3.14. *An algebraic extension $L|K$ is normal if the minimal polynomial over K of any element of L splits in L.*

Examples.

(1) The extension $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not normal. Indeed, the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ (to see this, notice that $x^3 - 2$ is irreducible my Eisenstein's criterion and that it annihilates $\sqrt[3]{2}$). On the other hand $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and $x^3 - 2$ has non real roots, so it does not split $\mathbb{Q}(\sqrt[3]{2})$.

(2) The extension $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is normal. Let $a \in \mathbb{Q}(\sqrt{2})$ and let $m_a(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (see note after Proposition 3.9), we have $\deg(m_a(x)) \leq 2$. On the other hand $m_a(x)$ has a root in $\mathbb{Q}(\sqrt{2})$, and any polynomial of degree ≤ 2, which has a root, splits. Hence $m_a(x)$ splits in $\mathbb{Q}(\sqrt{2})$.

Lemma 3.15. *Let $M = K(\alpha_1, \ldots, \alpha_k)|K$ be an algebraic field extension. Let $J|K$ be an extension in which the polynomial $\prod_{i=1}^{k} m_{\alpha_i}(x) \in K[x]$ splits (where $m_{\alpha_i}(x)$ is the minimal polynomials of α_i). Then there is a map of K-extensions $M \to J$. Furthermore, the number of maps of K-extensions $M \to J$ is finite. Finally, if the polynomials m_{α_i} are all separable, then there are $[M : K]$ such maps.*

In other words: the set of extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$ is finite and non empty, and if all the m_{α_i} are separable, then this set has cardinality $[M : K]$.

Proof. We prove the first and the second assertion together. According to Corollary 3.10, there is an extension of the map $K \hookrightarrow J$ to $K(\alpha_1)$, and there are only finitely many such extensions (since each extension corresponds to a root of m_{α_1} in J). Now note that the minimal polynomial of α_2 over $K(\alpha_1)$ divides $m_{\alpha_2}(x)$; it thus has a root in J, since $m_{\alpha_2}(x)$ splits in J. Thus we conclude again from Corollary 3.10 that for any ring map $K(\alpha_1) \hookrightarrow J$, there is an extension of this map to a map $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \hookrightarrow J$, and that there are only finitely many such extensions. Continuing this way, we see that there is an extension of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \ldots, \alpha_k) = M \hookrightarrow J$, and that there are only finitely many such extensions.

We now prove the third assertion. We repeat the reasoning we just made, computing degrees along the way. According to Corollary 3.10, there are $[K(\alpha_1) : K] = \deg(m_{\alpha_1(x)})$ extensions of the map $K \hookrightarrow J$ to $K(\alpha_1)$ (apply Corollary 3.4 and note that $m_{\alpha_1}(x)$ has no multiple roots). Similarly, for any ring map $K(\alpha_1) \hookrightarrow J$, there are $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ extensions of this map to a map $K(\alpha_1, \alpha_2) \hookrightarrow J$. Hence, by the tower law, there are

$$[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \alpha_2) \hookrightarrow J$. Continuing this way, we see that there are

$$[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1, \alpha_2)] \cdots [M : K(\alpha_1, \ldots, \alpha_{k-1})] = [M : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$. □

Theorem 3.16. *A finite field extension $L|K$ is normal iff it is a splitting extension for a polynomial with coefficients in K.*

Proof. Suppose that $L|K$ is finite and normal. Let $\alpha_1, \ldots, \alpha_k$ be generators for L over K (eg a K-basis). Let

$$P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K. Then, by assumption, $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field of $P(x)$.

Suppose now that L is a splitting field of a polynomial in $K[x]$. Let $\alpha \in L$ and let $\beta_1, \ldots, \beta_k \in L$ be st $L = K(\alpha, \beta_1, \ldots, \beta_k)$. Let J be a splitting field of the product of the minimal polynomials over K over the elements $\alpha, \beta_1, \ldots, \beta_k$. Now choose a root ρ in J of the minimal polynomial $Q(x)$ of α over K. We deduce from Corollary 3.10 that there is an extension of the map $K \hookrightarrow J$ to a ring map $\mu : K(\alpha) \hookrightarrow J$ such that $\mu(\alpha) = \rho$. Notice that by Lemma 3.15 there is an extension of μ to a ring map $\lambda : L \hookrightarrow J$. Now note that by Theorem 3.13 (iii), the image by λ of L in J is independent of λ, and thus of μ. Hence the image by λ of L in J contains all the roots of $Q(x)$, ie $Q(x)$ splits in the image of λ. Since $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ, we see that $Q(x)$ splits in L, which is what wanted to prove. □

Theorem 3.17. *Let $L|K$ be the splitting field of a separable polynomial over K. Then we have $\#\mathrm{Aut}_K(L) = [L : K]$.*

Proof. Apply Lemma 3.15 with $L = M = J$. □

Theorem 3.18. *Let $\iota : K \hookrightarrow L$ be a finite field extension. Then $\mathrm{Aut}_K(L)$ is finite. Furthermore, the following statements are equivalent*

(i) $\iota(K) = L^{\mathrm{Aut}_K(L))}$;

(ii) $L|K$ is normal and separable;

(iii) $L|K$ is a splitting extension for a separable polynomial with coefficients in K.

Proof. The fact that $\mathrm{Aut}_K(L)$ is finite is a consequence of the second assertion in Lemma 3.15 (if $\mathrm{Aut}_K(L)$ were infinite, then there one could obtain infinitely many maps of K-extensions $L \hookrightarrow J$ by composing a given map $L \hookrightarrow J$ with the elements of $\mathrm{Aut}_K(L)$).

(i)⇒(ii) Let $P(x)$ be the minimal polynomial of the element $\alpha \in L$. We have to show that $P(x)$ splits and is separable. Let

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\mathrm{Aut}_K(L),\alpha)} (x - \beta)$$

By construction, $Q(x)$ is separable. Let $d := \#\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Let $\beta_1, \ldots, \beta_d$ be the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. We have

$$Q(x) = x^d - s_1(\beta_1, \ldots, \beta_d)x^{d-1} + \cdots + (-1)^d s_d(\beta_1, \ldots, \beta_d)$$

Now note that for any $\gamma \in \mathrm{Aut}_K(L))$ and any $i \in \{1, \ldots, d\}$, we have

$$\gamma(s_i(\beta_1, \ldots, \beta_d)) = s_i(\gamma(\beta_1), \ldots, \gamma(\beta_d))$$

and thus, since s_i is a symmetric function and γ permutes the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$, we have

$$s_i(\gamma(\beta_1), \ldots, \gamma(\beta_d)) = s_i(\beta_1, \ldots, \beta_d).$$

Since γ was arbitrary, we see that $s_i(\beta_1, \ldots, \beta_d) \in L^G = \iota(K)$. Thus $Q(x) \in \iota(K)[x]$. Abusing language, we identify $Q(x)$ with a polynomial in $K[x]$ via ι. On the other hand $\alpha \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ so that $Q(\alpha) = 0$. Thus, by the definition of $P(x)$, we see that $P(x)$ divides $Q(x)$. Hence $P(x)$ splits in L and has no multiple roots. In particular, it is separable.

(ii)⇒(iii) Let $\alpha_1, \ldots, \alpha_k$ be generators of L over K. Let $P(x) := \prod_{i=1}^k m_{\alpha_i}(x)$, where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K. Then $P(x)$ is a separable polynomial by construction. On the other hand, L is a splitting field for $P(x)$, so we are done.

(iii)⇒(i) Note first that, by construction, $L^{\mathrm{Aut}_K(L)}$ contains the image of K (since any element of $\mathrm{Aut}_K(L)$ fixes the image of K in L by definition). In other words, the extension $L|K$ is the composition of an extension $L^{\mathrm{Aut}_K(L))}|K$ and $L|L^{\mathrm{Aut}_K(L)}$. Note that the extension $L|L^{\mathrm{Aut}_K(L)}$ is also the splitting field of a separable polynomial over $L^{\mathrm{Aut}_K(L)}$ (take the same polynomial as for $L|K$ and apply the remark following Lemma 3.6). Also, notice that, tautologically, the subgroup $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) \subseteq \mathrm{Aut}_K(L)$ actually coincides with $\mathrm{Aut}_K(L)$.

Now, using Theorem 3.17, we may compute that

$$[L : L^{\mathrm{Aut}_K(L)}] = \#\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L))$$

and

$$[L : K] = \#\mathrm{Aut}_K(L))$$

so that $[L : L^{\mathrm{Aut}_K(L)}] = [L : K]$. We conclude from the tower law that $[L^{\mathrm{Aut}_K(L)} : K] = 1$, ie

$$L^{\mathrm{Aut}_K(L)} = \iota(K).$$

□

Corollary 3.19. *Let $L|K$ be an algebraic field extension. Suppose that L is generated by $\alpha_1, \ldots, \alpha_k \in M$ and that the minimal polynomial of each α_i is separable. Then the extension $L|K$ is separable.*

Proof. According to Lemma 3.15 and Theorem 3.13, there is an extension $M|L$ st the extension $M|K$ is the splitting field of a separable polynomial. According to Theorem 3.18, the extension $M|K$ is separable. Thus, by Lemma 3.8 (or by definition), the extension $L|K$ is also separable. □

END OF LECTURE 5

4 Galois extensions

4.1 Overview

Definition 4.1. *A field extension $\iota : K \hookrightarrow L$ is called a Galois extension, if $L^{\mathrm{Aut}_K(L)} = \iota(K)$.*

In the rest of these notes, we shall often drop the map ι in our computations and identify $\iota(K)$ with K (but only when it does not lead to any ambiguity).

Note. By Theorem 3.18, a finite field extension $L|K$ is a Galois extension iff L is the splitting field of a separable polynomial over K and iff it is normal and separable. From this, we see that if $L|K$ is finite Galois extension, which is the composition of two extensions $L|K_1$ and $K_1|K$, then $L|K_1$ is also a finite Galois extension. However, it is not true in general that $K_1|K$ is then also a Galois extension. More about this in Theorem 4.4 (iii) below.

If $L|K$ is a Galois extension, we write

$$\mathrm{Gal}(L|K) = \Gamma(L|K) := \mathrm{Aut}_K(L)$$

and we call $\mathrm{Gal}(L|K)$ the *Galois group* of $L|K$. If $L|K$ is a finite, then this is a finite group. This follows from Theorem 3.18 and from Theorem 3.17 (or directly from the reasoning made at the very beginning of these notes).

Let K be a field and $P(x) \in K[x]$ a separable polynomial. Let $L|K$ be a splitting field for $P(x)$. We shall sometimes write $\mathrm{Gal}(P) = \mathrm{Gal}(P(x))$ for $\mathrm{Gal}(L|K)$. Note however that this is an abuse of notation, because the various splitting fields of $P(x)$ are not related by *canonical* isomorphisms. Thus, stricto sensu, $\mathrm{Gal}(P)$ can only refer to an isomorphism class of finite groups, and not a particular group.

Fundamental theorem of Galois theory (to be proven later in a more detailed form). The map

$$\{\text{subfields of } L \text{ containing } \iota(K)\} \mapsto \{\text{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection.

Example. We shall compute the Galois group of the extension $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ and of its subfields. Note that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the polynomial $(x^2-2)(x^2+1)$, whose roots are $\pm\sqrt{2}, \pm i$. Thus $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ is the splitting field of a separable polynomial, and is thus Galois.

We have successive extensions $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ (it annihilates $\sqrt{2}$, and it is irreducible, since it is of degree 2 and has no roots in $\mathbb{Q}$). Similarly, the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$ (it annihilates i, and it is irreducible, since it is of degree 2 and has no roots in $\mathbb{Q}(\sqrt{2})$, as $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$). Thus we conclude from the tower law and the note after Proposition 3.9 that $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 2 \cdot 2 = 4$. Now we deduce from Theorem 3.17 that $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}) = 4$. Let $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q})$. From the classification of finite groups (we shall come back to this later in the course), we conclude that G is abelian. Further, from the structure theorem for finite abelian groups (see Rings and Modules), we see that we either have $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G = \mathbb{Z}/4\mathbb{Z}$. Now note that we have $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) = 2$. This follows from the fact that

the extension $\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(i)$ is not trivial (otherwise, $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]$ would be equal to 2, by the tower law). Similarly, $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(\sqrt{2}))=2$. Since the only group of order 2 is $\mathbb{Z}/2\mathbb{Z}$, we conclude that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(i))\simeq\mathbb{Z}/2\mathbb{Z}$ and that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(\sqrt{2}))\simeq\mathbb{Z}/2\mathbb{Z}$.

Now note that by the fundamental theorem of Galois theory (above), the subgroups $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(\sqrt{2}))\subseteq G$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}(i))\subseteq G$ cannot coincide, because they correspond to different subfields of $\mathbb{Q}(\sqrt{2},i)$. Thus we conclude that G has two distinct subgroups of order 2, and hence we must have $G\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Altogether, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ has three non trivial subgroups, which are all of order 2: $\mathbb{Z}/2\mathbb{Z}\times\{0\}$, $\{0\}\times\mathbb{Z}/2\mathbb{Z}$ and the subgroup generated by $(1 \pmod 2), 1 \pmod 2)$. We conclude that $\mathbb{Q}(\sqrt{2},i)$ contains three non trivial subfields (note that any field of characteristic 0 contains $\mathbb{Q}$, so we need not worry about the condition that the subfields contain $\mathbb{Q}$ here). We have already found two of them ($\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$). A third subfield is given by $\mathbb{Q}(i\sqrt{2})$. We clearly have $\mathbb{Q}(\sqrt{2})\neq\mathbb{Q}(i\sqrt{2})$ and we also have $\mathbb{Q}(i)\neq\mathbb{Q}(i\sqrt{2})$, for otherwise $\sqrt{2}$ would lie in $\mathbb{Q}(i)$ and we have already seen that $\mathbb{Q}(\sqrt{2})\neq\mathbb{Q}(i)$. This completes the description of the Galois correspondence for $\mathbb{Q}(\sqrt{2},i)|\mathbb{Q}$.

Examples of field extensions, which are not Galois.

(i) We saw at the beginning of subsection 3.5 that $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not a normal extension. Thus it is not Galois.

(ii) Consider the extension $\mathbb{F}_2(t)[x]/(x^2-t)|\mathbb{F}_2(t)$. We saw at the end of subsection 3.2 that this extension is not separable. Thus it is not Galois (by Theorem 3.18).

END OF LECTURE 6

4.2 Artin's lemma

Artin's lemma is the following basic statement, which is the linchpin of the whole theory.

Theorem 4.2 (Artin's lemma)**.** *Let K be a field and let $G\subseteq\mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then the extension $K|K^G$ is a finite Galois extension, and the inclusion $G\hookrightarrow\mathrm{Aut}_{K^G}(K)$ is an isomorphism of groups.*

Note. The key point of Artin's lemma is the fact that $K|K^G$ is a finite extension. This is proven in Lemma 4.3 below.

Lemma 4.3. *Let K be a field and let $G\subseteq\mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then $[K:K^G]\leq\#G$.*

Proof. Suppose not. Then there is a sequence $\alpha_1\ldots,\alpha_d$ of elements of K, which is linearly independent over K^G and such that $d>\#G$. Let $n:=\#G$ and let $\sigma_1,\ldots,\sigma_n\in G$ be an enumeration of the elements of G. Consider the matrix

$$\begin{bmatrix}\sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_d)\\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_d)\\ \vdots & \vdots & \ddots & \vdots\\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_d)\end{bmatrix}$$

Note that the columns of this matrix are linearly dependent over K (because $n<d$). So there exists a sequence $\beta_1\ldots,\beta_d\in K$, where at least one β_i does not vanish, st

$$\sum_{i=1}^{d}\beta_i\sigma_k(\alpha_i)=0 \tag{1}$$

for all $k \in \{1, \dots, n\}$. Choose the sequence $\beta_1 \dots, \beta_d$ so that the quantity

$$r := \#\{i \in \{1, \dots \mathrm{d}\} \,|\, \beta_i \neq 0\}$$

is minimal. Renumbering, we may suppose that $\beta_1, \dots, \beta_r \neq 0$ and that $\beta_{r+1} = \beta_{r+2} = \dots = \beta_d = 0$. Dividing by β_r, we may suppose that $\beta_r = 1$. Note now that, by the assumption that the $\alpha_1 \dots, \alpha_d$ are linearly independent over K^G, there exists $i_0 \in \{1, \dots, r\}$ st $\beta_{i_0} \notin K^G$ (in particular, we have $r > 1$, since $i_0 \neq r$). Renumbering again, we may assume that $\beta_1 \notin K^G$.

Let now $k_0 \in \{1, \dots, n\}$ be st $\sigma_{k_0}(\beta_1) \neq \beta_1$. Applying σ_{k_0} to the equations (1), we see that

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)(\sigma_{k_0}\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. In other words, we have

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)\sigma_k(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. Subtracting the equations in (1) from these equations, we obtain

$$\sum_{i=1}^{d} (\sigma_{k_0}(\beta_i) - \beta_i)\sigma_k(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. In view of the definition of r and of the fact that $\beta_r = 1$, this equivalent to writing that

$$\sum_{i=1}^{r-1} (\sigma_{k_0}(\beta_i) - \beta_i)\sigma_k(\alpha_i) = 0$$

for all $k \in \{1, \dots, n\}$. However, since $\sigma_{k_0}(\beta_1) \neq \beta_1$, this contradicts the minimality of r. We conclude that we cannot have $d > n$, which is what we wanted to prove. □

We are now in a position to prove Artin's lemma.

Proof. (of Theorem 4.2) We shall first prove that

$$K^G = (K)^{\mathrm{Aut}_{K^G}(K)}$$

We have $K^G \subseteq (K)^{\mathrm{Aut}_{K^G}(K)}$ by definition. On the other hand, we have $G \subseteq \mathrm{Aut}_{K^G}(K)$, again by definition, so that $K^G \supseteq (K)^{\mathrm{Aut}_{K^G}(K)}$. We conclude that $K^G = (K)^{\mathrm{Aut}_{K^G}(K)}$, as required. Now, *since* $K|K^G$ *is a finite extension* by Lemma 4.3, we can conclude from Theorem 3.18 that $K|K^G$ is a splitting extension of a separable polynomial with coefficients in K^G. We may thus conclude from Theorem 3.17 that

$$[K : K^G] = \#\mathrm{Aut}_{K^G}(K).$$

On the other hand, we know from Lemma 4.3 that $[K : K^G] \leq \#G$, so that $\#\mathrm{Aut}_{K^G}(K) \leq \#G$. Since $G \subseteq \mathrm{Aut}_{K^G}(K)$, we also have $\#G \leq \#\mathrm{Aut}_{K^G}(K)$, and we conclude that $\#G = \#\mathrm{Aut}_{K^G}(K)$. This implies that $G = \mathrm{Aut}_{K^G}(K)$. Now Theorem 3.18 implies that $K|K^G$ is a finite Galois extension with Galois group G. □

END OF LECTURE 7

4.3 The fundamental theorem of Galois theory

If $\iota : K \hookrightarrow L$ is a field extension, we shall call a subfield of L containing $\iota(K)$ an *intermediate field*.

Theorem 4.4. *Let $\iota : K \hookrightarrow L$ be a finite Galois extension.*

(i) The map

$$\{\textit{subfields of } L \textit{ containing } \iota(K)\} \mapsto \{\textit{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection. Its inverse is given by the map

$$H \mapsto L^H.$$

(where H is a subgroup of $\mathrm{Gal}(L|K)$).

We shall write $G_M := \mathrm{Gal}(L|M)$.

(ii) Let M be a subfield of L containing $\iota(K)$. We have

$$[L : M] = \#G_M$$

and

$$[M : K] = \frac{\#\mathrm{Gal}(L|K)}{\#G_M}$$

(iii) Let M be a subfield of L containing $\iota(K)$. Then $M|K$ is a Galois extension iff the group G_M is a normal subgroup of $\mathrm{Gal}(L|K)$. If that is the case, there is an isomorphism $I_M : \mathrm{Gal}(L|K)/G_M \simeq \mathrm{Gal}(M|K)$, which is uniquely determined by the fact that $I_M(\gamma \pmod{G_M}) = \gamma|_M$ for any $\gamma \in \mathrm{Gal}(L|K)$. Here $\gamma|_M$ is the restriction of γ to M and it is part of the statement that $\gamma(M) = M$.

Proof. (i) We need to prove that $M = L^{G_M}$ and $G_{L^H} = H$ for any intermediate field M and any subgroup $H \subseteq \mathrm{Gal}(L|K)$.

We first prove that $M = L^{G_M}$. This is simply a consequence of the fact that $L|M$ is a Galois extension (see the beginning of subsection 4.1).

We now prove that $G_{L^H} = H$. This is the content of Artin's lemma applied to L and H.

(ii) The equation $[L : M] = \#G_M$ is a consequence of Theorem 3.17. The equation $[M : K] = \#\mathrm{Gal}(L|K)/\#G_M$ is a consequence of the tower law and of the fact that $\#\mathrm{Gal}(L|K) = \#G_K = [L : K]$.

(iii) Suppose that M is an intermediate field and that $M|K$ is a Galois extension. Then for all $\gamma \in \mathrm{Gal}(L|K)$, we have $\gamma(M) = M$. This is a consequence of Theorem 3.13 (iii). In particular, there is a homomorphism

$$\phi_M : \mathrm{Gal}(L|K) \to \mathrm{Gal}(M|K)$$

given by the formula $\phi(\gamma) = \gamma|_M$. The kernel of this homomorphism is G_M by definition. Hence G_M is normal in $\mathrm{Gal}(L|K)$ by the first isomorphism theorem.

Suppose now that G_M is a normal subgroup of $\mathrm{Gal}(L|K)$. Let $\gamma \in \mathrm{Gal}(L|K)$. We compute from the definitions

$$\begin{aligned} & G_{\gamma(M)} = \mathrm{Gal}(L|\gamma(M)) = \{\mu \in \mathrm{Gal}(L|K) \,|\, \mu(\alpha) = \alpha, \forall \alpha \in \gamma(M)\} \\ = \; & \{\mu \in \mathrm{Gal}(L|K) \,|\, \mu(\gamma(\beta)) = \gamma(\beta), \forall \beta \in M\} \\ = \; & \{\mu \in \mathrm{Gal}(L|K) \,|\, (\gamma^{-1}\mu\gamma)(\beta)) = \beta, \forall \beta \in M\} \\ = \; & \gamma G_M \gamma^{-1} \\ = \; & G_M \end{aligned}$$

By (i), we conclude that $\gamma(M) = M$. Thus, we again have a homomorphism

$$\phi_M : \mathrm{Gal}(L|K) \to \mathrm{Aut}_K(M)$$

given by the formula $\phi(\gamma) = \gamma|_M$. From (ii) and the first isomorphism theorem, we conclude that the image $\mathrm{Im}(\phi_M) \subseteq \mathrm{Aut}_K(M)$ of ϕ_M has cardinality $[M : K]$. On the other hand, by Artin's lemma, Theorem 3.18 and Theorem 3.17, we know that $[M : M^{\mathrm{Im}(\phi_M)}] = \#\mathrm{Im}(\phi_M)$ so that $[M : M^{\mathrm{Im}(\phi_M)}] = [M : K]$. So the tower law implies that $K = M^{\mathrm{Im}(\phi_M)}$. In particular, $M|K$ is a Galois extension and the map ϕ_M is surjective. The map I_M is obtained directly from the map ϕ_M and the first isomorphism theorem. □

Note. Here is an important characterisation of Galois extensions, which was established in the course of (iii) above (and it also a consequence of it). Let $\iota : K \hookrightarrow L$ be a Galois extension. Let $M \subseteq L$ be an intermediate field. Then $M|K$ is a Galois extension iff all the maps of K-extensions $M \to L$ have the same image (which must be M). Indeed, suppose that all the maps of K-extensions $M \to L$ have M has an image. Then for all $\gamma \in \mathrm{Gal}(L|K)$, we have $\gamma(M) = M$ and thus from (iii) above (see its proof for details), $M|K$ is a Galois extension. On the other hand, if $M|K$ is a Galois extension, then for all $\gamma \in \mathrm{Gal}(L|K)$, we must have $\gamma(M) = M$ by Theorem 3.13 and Theorem 3.18 (iii).

Corollary 4.5 (of Theorem 4.4)**.** *Let $\iota : K \hookrightarrow L$ be a finite separable extension. Then there are only finitely many intermediate fields between L and $\iota(K)$.*

Proof. We may wrog replace L by one of its extensions. By Lemma 3.15, Theorem 3.18 and the existence of splitting fields, we may thus suppose that the extension $L|K$ is a Galois extension. In that case, the statement is a consequence of Theorem 4.4 (i) and the fact that $\mathrm{Gal}(L|M)$ is finite (and thus has finitely many subgroups). □

END OF LECTURE 8

We record the following important lemmata, the first of which could have already been proven right after Theorem 3.18.

Lemma 4.6. *Let $L|K$ be a finite Galois extension. Let $\alpha \in L$. Then the minimal polynomial of α over K is the polynomial*

$$\prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K), \alpha)} (x - \beta)$$

Proof. Let $P(x) = \prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K),\alpha)}(x-\beta)$. We have already seen part of the argument in the proof of Theorem 3.18. Let $m_\alpha(x) \in K$ be the minimal polynomials of α over K. We saw at the beginning of the proof of Theorem 3.18 that $P(x) \in K[x]$. Thus, by the definition of the minimal polynomial, we have

$$m_\alpha(x)|P(x).$$

To conclude the proof, we only need to prove that $P(x)$ is irreducible over K. Suppose for contradiction that $P(x)$ is not irreducible and let $P(x) = Q(x)T(x)$, where $Q(x), T(x) \in K[x]$ and $\deg(Q), \deg(T) > 1$. Note that if $\rho \in L$ and $Q(\rho) = 0$, then for any $\gamma \in \mathrm{Gal}(L|K)$, we have

$$\gamma(Q(\rho)) = Q(\gamma(\rho)) = \gamma(0) = 0$$

and thus the roots of $Q(x)$ in L are stable under the action of $\mathrm{Gal}(L|K)$. Now note that $Q(x)$ has a root in L, since $P(x)$ splits in L and $Q(x)|P(x)$. Thus the set of the roots of $P(x)$ contains a subset, which is stable under $\mathrm{Gal}(L|K)$ and has cardinality strictly smaller than $\deg(P(x)) = \#\mathrm{Orb}(\mathrm{Gal}(L|K), \alpha)$. This contradicts the fact that the set of roots of $P(x)$ is the orbit of α under $\mathrm{Gal}(L|K)$. $\square$

We shall need the following group-theoretic terminology in the following lemma. Let $n \geq 1$. A finite subgroup G of S_n is called *transitive* if it has only one orbit in $\{1, \ldots, n\}$.

Lemma 4.7. *Let K be a field and let $P(x) \in K[x]$. Let $L|K$ be a splitting extension of $P(x)$ and let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $P(x)$, with multiplicities.*

(1) Suppose that $P(x)$ has no repeated roots. Let $\phi : \mathrm{Aut}_K(L) \to S_n$ be the map st $\gamma(\alpha_i) = \alpha_{\phi(\gamma)(i)}$ for all $i \in \{1, \ldots, n\}$. Then ϕ is an injective group homomorphism.

(2) If $P(x)$ is irreducible over K and has no repeated roots, then the image of ϕ is a transitive subgroup of S_n.

(3) The element $\Delta_P := \Delta(\alpha_1, \ldots, \alpha_n)$ lies in K and depends only on $P(x)$.

(4) Suppose that $\mathrm{char}(K) \neq 2$. Suppose that $P(x)$ has no repeated roots. Then the image of ϕ lies inside $A_n \subseteq S_n$ iff $\Delta_P \in (K^*)^2$.

Here the set $(K^*)^2$ is the set of non zero squares in K. The polynomial $\Delta(x_1, \ldots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x]$ was defined in Proposition-Definition 2.17.

Proof. (1) The map ϕ is a tautologically a group homomorphism. It is injective, because L is generated by $\alpha_1, \ldots, \alpha_n$ and thus an element $\gamma \in \mathrm{Aut}_K(L)$, which acts as the identity on the set $\alpha_1, \ldots, \alpha_n$, must act as the identity on L.

(2) We need to show that $\mathrm{Aut}_K(L)$ acts transitively on the set $\alpha_1 \ldots, \alpha_n$. Now, since $P(x)$ is irreducible, it is the minimal polynomial of any of the α_i. Now apply Lemma 4.6.

(3) Note that

$$P(x) =: x^d + a_{d-1}x^{d-1} + \cdots + a_0 = x^d - \sigma_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \sigma_2(\alpha_1, \ldots, \alpha_d)x^{d-2} + - \cdots + (-1)^d\sigma_d(\alpha_1, \ldots, \alpha_d)$$

(see before Theorem 2.16). On the other hand, by Theorem 2.16, there is a unique polynomial $Q(x) \in K[x]$ st $Q(s_1, \ldots, s_d) = \Delta(x_1, \ldots, x_d)$. Hence

$$\Delta(\alpha_1, \ldots, \alpha_n) = Q(-a_{d-1}, a_{d-2}, \ldots, (-1)^d a_0)$$

Since $Q(-a_{d-1}, a_{d-2}, \ldots, (-1)^d a_0)$ depends only on $P(x)$ and lies in K, we are done.

(4) Consider the expression $\delta(\alpha_1, \ldots, \alpha_n) := \prod_{i<j}(\alpha_i - \alpha_j)$. Using Proposition-Definition 2.17, we compute that for any $\gamma \in \mathrm{Aut}_K(L)$, we have

$$\gamma(\delta(\alpha_1, \ldots, \alpha_n)) = \delta(\gamma(\alpha_1), \ldots, \gamma(\alpha_n)) = \delta(\alpha_{\phi(\gamma)(1)}, \ldots, \alpha_{\phi(\gamma)(n)}) = \mathrm{sign}(\phi(\gamma)) \cdot \delta(\alpha_1, \ldots, \alpha_n)$$

Thus $\delta(\alpha_1, \ldots, \alpha_n) \in K$ iff the image of ϕ lies inside A_n. Now note that $\delta(\alpha_1, \ldots, \alpha_n) \in K$ iff $\Delta_P \in (K^*)^2$. $\square$

Note the trivial fact that $\Delta_P = 0$ iff $P(x)$ has repeated roots.

Example. In the first exercise sheet, it is shown that

$$\Delta(x_1, x_2, x_3) = -4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3 - 4s_2^3 - 27 s_3^2$$

(where the s_i are the symmetric functions in 3 variables). Now let $P(x) = x^3 - x - \frac{1}{3} \in \mathbb{Q}[x]$. The polynomial $P(x)$ has no roots in $\mathbb{Q}$ (exercise) and it thus irreducible over $\mathbb{Q}$. In particular, it has no multiple roots, since $\mathrm{char}(\mathbb{Q}) = 0$ (see after Lemma 3.6). Let $L|\mathbb{Q}$ be a splitting field for $P(x)$ and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $P(x)$ in L. We have $s_3(\alpha_1, \alpha_2, \alpha_3) = -1/3$, $s_2(\alpha_1, \alpha_2, \alpha_3) = -1$ and $s_1(\alpha_1, \alpha_2, \alpha_3) = 0$. In particular,

$$\Delta_P = -4 s_2(\alpha_1, \alpha_2, \alpha_3)^3 - 27 s_3(\alpha_1, \alpha_2, \alpha_3)^2 = 4 - \frac{27}{9} = 1$$

Thus $\Delta_P \in (\mathbb{Q}^*)^2$ (this gives another proof of the fact that $P(x)$ has no repeated roots). We conclude from Lemma 4.7 (4) that $\mathrm{Gal}(L|\mathbb{Q})$ can be realised as a subgroup of A_3. Furthermore, we know that $\mathrm{Gal}(L|\mathbb{Q})$ has at least order 3 because the extension $K(\alpha_i)|\mathbb{Q}$ has degree 3 for any α_i. The fact that the extension $K(\alpha_i)|\mathbb{Q}$ has degree 3 follows from Proposition 3.9 and from the fact that $P(x)$ irreducible, and is thus the minimal polynomial of α_i. The fact that $\mathrm{Gal}(L|\mathbb{Q})$ has at least order 3 now follows from the tower law and Theorem 3.17.

Since $\# A_3 = 3$, we conclude that $\mathrm{Gal}(L|\mathbb{Q}) \simeq A_3$.

4.4 The theorem of the primitive element

Theorem 4.8. *Let $L|K$ be a finite separable extension of fields. Then there is an element $\alpha \in L$ st $L = K(\alpha)$.*

Proof. We suppose that K is an infinite field. The case of a finite field is treated in the exercises. Since L is a finite extension of K, L is generated over K by a finite number of elements. By induction on the number of generators, it will be sufficient to prove that L is generated by one element if it is generated by two elements. So suppose that $L = K(\beta, \gamma)$. For $d \in K$, we consider the intermediate field $K(\beta + d\gamma)$. By Corollary 4.5 there are only finitely many intermediate fields. Since K is infinite, we may thus find $d_1, d_2 \in K$ such that $d_1 \neq d_2$ and $K(\beta + d_1\gamma) = K(\beta + d_2\gamma)$. By Proposition 3.9, there is thus a polynomial $P(x) \in K[x]$ st $\beta + d_1\gamma = P(\beta + d_2\gamma)$. Thus we have

$$\gamma = \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and

$$\beta = (\beta + d_2\gamma) - d_2 \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and in particular

$$K(\beta, \gamma) = K(\beta + d_2\gamma).$$

□

END OF LECTURE 9

5 Special classes of extensions

5.1 Cyclotomic extensions

Let $n \geq 1$. For any field E, define

$$\mu_n(E) := \{\rho \in E \,|\, \rho^n = 1\}.$$

Note that the set $\mu_n(E)$ inherits a group structure from E^*. The elements of $\mu_n(E)$ are called the *n-th roots of unity* (in E).

Lemma 5.1. *The group $\mu_n(E)$ is a finite cyclic group.*

Proof. Exercise. Use the fact that a finite commutative group G is cyclic iff for any divisor $d|\#G$, there is at most one subgroup in G, which has cardinality $\#G$. □

If $\#\mu_n(E) = n$, we shall call an element $\omega \in \mu_n(E)$ a *primitive* n-th root of unity if it is a generator of $\mu_n(E)$ (if $\#\mu_n(E) \neq n$ then this terminology is not used). Note that if $\omega \in \mu_n(E)$ is a primitive n-th root of unity, then all the other primitive n-th roots of unity are of the form ω^k, where k is an integer prime to $\#\mu_n(E)$.

We will also need the

Lemma 5.2. *Let G be a finite cyclic group. Write the group law of G multiplicatively. Let $k := \#G$. Let $I : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ be the map given by the formula $I(a \pmod k)(\gamma) = \gamma^a$ for any $a \in \mathbb{Z}$ and $\gamma \in G$. Then I is an isomorphism.*

Proof. Exercise. □

Let now K be a field and suppose that $(n, \mathrm{char}(K)) = (1)$.

Let L be a splitting field for the polynomial $x^n - 1 \in K[x]$. Abusing language, we shall in the following sometimes denote such a splitting field by $K(\mu_n)$ (we abuse language, because L is only well-defined up to isomorphism). Note that $x^n - 1$ has no repeated roots, because $\frac{\mathrm{d}}{\mathrm{d}x}(x^n - 1) = nx^{n-1} \neq 0$ (see subsection 3.2). Thus $\#\mu_n(L) = n$ and $L|K$ is a Galois extension. In particular, since $\mu_n(L) \simeq \mathbb{Z}/n\mathbb{Z}$ by Lemma 5.1, we see that there are $\#(\mathbb{Z}/n\mathbb{Z})^* = \Phi(n)$ primitive n-th roots of unity in L. Here $\Phi(\bullet)$ is Euler's totient function.

Let

$$\Phi_{n,K}(x) := \prod_{\omega \in \mu_n(E),\, \omega \text{ primitive}} (x - \omega)$$

Note that $\deg(\Phi_{n,K}(x)) = \Phi(n)$. Also, note that $L|K$ is a simple extension, because L is generated over K by any primitive n-th root of unity in L.

Lemma 5.3. *The polynomial $\Phi_{n,K}(x)$ has coefficients in K and depends only on n and K.*

Proof. The coefficients of $\Phi_{n,K}(x)$ are symmetric functions in the primitive $n-$th roots. Since the primitive n-roots are permuted by $\mathrm{Gal}(L|K)$, the coefficients are thus invariant under $\mathrm{Gal}(L|K)$, and thus lies in K. The polynomial $\Phi_{n,K}(x) \in K[x]$ only depends on n and K, because all the splitting K-extensions for $x^n - 1$ are isomorphic by Theorem 3.13 (ii). $\square$

Proposition 5.4. *(i) There is a natural injection of groups $\phi : \mathrm{Gal}(L|K) \hookrightarrow \mathrm{Aut}_{\mathrm{Groups}}(\mu_n(L))$.*

(ii) The map ϕ is surjective iff $\Phi_{n,K}(x)$ is irreducible over K.

From Lemma 5.2, we see that we have in particular a canonical injection of groups $\phi : \mathrm{Gal}(L|K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (i) is clear, since $\mu_n(L)$ generates L and $\mathrm{Gal}(L|K)$ acts on L by ring automorphisms.

(ii) Let $\omega \in \mu_n(L)$ be a primitive n-th root of unity. Suppose that $\Phi_{n,K}(x)$ is irreducible over K. Since $\Phi_{n,K}(x)$ annihilates ω, it must be the minimal polynomial of ω. Hence $[L : K] \geq \Phi(n)$ (by Proposition 3.9), and thus we have $\#\mathrm{Gal}(L|K) \geq \Phi(n)$ by Theorem 3.17. On the other hand $\#\mathrm{Gal}(L|K) \leq \Phi(n)$ by (i) and Lemma 5.2. Hence $\#\mathrm{Gal}(L|K) = \Phi(n)$ and we may conclude from (i) that ϕ is surjective.

Now suppose that ϕ is surjective. Then the minimal polynomial of ω is $\Phi_{n,K}(x)$ by Lemma 5.2 and Lemma 4.6. $\square$

Proposition 5.5. *The polynomial $\Phi_{n,\mathbb{Q}}(x)$ is irreducible and has coefficients in $\mathbb{Z}$.*

Proof. Let L be a splitting field of $x^n - 1 \in \mathbb{Q}[x]$. Let $\omega \in L$ be a primitive n-th root of unity. Let $Q(x) \in \mathbb{Q}[x]$ be the minimal polynomial of ω over $\mathbb{Q}$. Then $Q(x)|x^n - 1$ and thus there is a polynomial $T(x) \in \mathbb{Q}[x]$ st $Q(x)T(x) = x^n - 1$. Note that $T(x)$ and $Q(x)$ are monic. Thus $1/c(T)$ and $1/c(Q)$ are both positive integers. Here $c(\bullet)$ is the Gauss content function, defined just before Lemma 2.13. On the other hand we compute that $c(x^n - 1) = 1$ and by Lemma 2.13, we know that

$$1 = c(T)c(Q)$$

and thus $c(T) = c(Q) = 1$. We conclude that $Q(x)$ and $T(x)$ have coefficients in $\mathbb{Z}$.

Let now be a prime number p, which is prime to n. We claim that $Q(\omega^p) = 0$. Suppose for contradiction that $Q(\omega^p) \neq 0$. Then we have $T(\omega^p) = 0$ since $Q(x)T(x) = x^n - 1$. In particular, ω is a root of $T(x^p)$. Thus $Q(x)|T(x^p)$. In other words, there is a polynomial $H(x) \in \mathbb{Q}[x]$ st $Q(x)H(x) = T(x^p)$. Note that $H(x)$ is also monic. Computing contents and applying Lemma 2.13 again, we see that $H(x) \in \mathbb{Z}[x]$. Now notice that

$$T(x^p) \,(\mathrm{mod}\ p) = (T(x) \,(\mathrm{mod}\ p))^p$$

in $\mathbb{F}_p[x]$ (because the p-power function is additive in $\mathbb{F}_p[x]$ - see Rings and Modules). Reducing mod p the equality $Q(x)H(x) = T(x^p)$, we conclude that $\gcd(Q(x) \,(\mathrm{mod}\ p), T(x), (\mathrm{mod}\ p)) \neq 1$. Let

$$J(x) := \gcd(Q(x) \,(\mathrm{mod}\ p), T(x) \,(\mathrm{mod}\ p)).$$

Since $Q(x)T(x) = x^n - 1$, we see that $J(x)^2 | x^n - 1 \,(\mathrm{mod}\ p)$ and we conclude that $x^n - 1 \,(\mathrm{mod}\ p)$ has multiple roots. However, we have $\frac{\mathrm{d}}{\mathrm{d}x}(x^n - 1) \,(\mathrm{mod}\ p) = nx^{n-1} \,(\mathrm{mod}\ p) \neq 0$ and so

$$(x^n - 1 \,(\mathrm{mod}\ p), nx^{n-1} \,(\mathrm{mod}\ p)) = (1).$$

This is a contradiction and we may thus conclude that $Q(\omega^p) = 0$.

Applying the claim for various primes numbers repeatedly, we see that $Q(\omega^k) = 0$ for any integer k, which is coprime to n. In other words, all the primitive n-th roots of unity are roots of $Q(x)$. Thus $\deg(Q) \geq \Phi(n)$. Finally, notice that by definition we have $Q(x)|\Phi_{n,\mathbb{Q}}(x)$. Since $\deg(\Phi_{n,\mathbb{Q}}(x)) = \Phi(n)$, we must have $Q(x) = \Phi_{n,\mathbb{Q}}(x)$. In particular, $\Phi_{n,\mathbb{Q}}(x)$ is irreducible and has coefficients in $\mathbb{Z}$. □

END OF LECTURE 10

5.2 Kummer extensions

Let K be a field and let n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K.

Let $a \in K$ and let $M|K$ be a splitting extension for the polynomial $x^n - a$. Note that $\frac{\mathrm{d}}{\mathrm{d}x}(x^n - a) = nx^{n-1}$. Since $(x^n - a, nx^{n-1}) = (1)$, we see that $x^n - a$ is a separable polynomial. Hence $M|K$ is a Galois extension. Such an extension is called a *Kummer* extension.

Lemma 5.6. *Let $\rho \in L$ be st that $\rho^n = a$. There is a unique group homomorphism $\phi : \mathrm{Gal}(M|K) \to \mu_n(K)$ st that $\phi(\gamma) = \gamma(\rho)/\rho$. This map does not depend on the choice of ρ and is injective.*

Proof. We compute $(\gamma(\rho)/\rho)^n = \gamma(\rho^n)/\rho^n = a/a = 1$ and thus we indeed have $\gamma(\rho)/\rho \in \mu_n(K)$. To see that the map does not depend on ρ, note that if $\rho_1^n = a$, then $(\rho/\rho_1)^n = a/a = 1$. Thus there is an n-th root of unity $\mu \in K$ st $\rho_1 = \mu\rho$. Now, using the fact that $x^n - 1$ splits in K, we may compute

$$\gamma(\rho)/\rho = \mu\gamma(\rho)/(\mu\rho) = \gamma(\mu\rho)/(\mu\rho) = \gamma(\rho_1)/\rho_1$$

so the function ϕ does not depend on ρ.

We now prove that ϕ is a group homomorphism. For any $\gamma, \lambda \in \mathrm{Gal}(M|K)$, we have by definition

$$\phi(\gamma\lambda) = \gamma(\lambda(\rho))/\rho$$

and

$$\phi(\gamma)\phi(\lambda) = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho)$$

and thus we have to prove that

$$\gamma(\lambda(\rho))/\rho = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho)$$

ie that

$$\gamma(\lambda(\rho)) = \lambda(\rho)\gamma(\rho)/\rho. \tag{2}$$

Now, again using the fact that $x^n - 1$ splits in K, we compute

$$\gamma(\lambda(\rho)/\rho) = \gamma(\lambda(\rho))/\gamma(\rho) = \lambda(\rho)/\rho. \tag{3}$$

Since equations (2) and 3 are equivalent, we have proven that ϕ is group homomorphism.

Finally the map ϕ is clearly injective, because any element of $\ker(\phi)$ would fix all the roots of $x^n - a$, and hence would fix K. □

The proof of the previous lemma also shows that a Kummer extension $M|K$ as above is a simple extension, generated by any root of $x^n - a$.

The following theorem is a kind of converse to Lemma 5.6.

Theorem 5.7. *Let K be a field and let n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K. Suppose that $L|K$ is a Galois extension and that $\mathrm{Gal}(L|K)$ is a cyclic group of order n.*

Let $\sigma \in \mathrm{Gal}(L|K)$ be a generator of $\mathrm{Gal}(L|K)$ and let $\omega \in K$ is a primitive n-th root of unity in K. For any $\alpha \in L$ let

$$\beta(\alpha) := \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha).$$

Then:

- for any $\alpha \in L$, we have $\beta(\alpha)^n \in K$;

- if $\beta(\alpha) \neq 0$, then $L = K(\beta)$ (so that L is the splitting field of $x^n - \beta(\alpha)^n$);

- there is an $\alpha \in L$, such that $\beta(\alpha) \neq 0$.

For the proof, we shall need a general result on characters of groups with values in multiplicative groups of fields.

Let E be a field. Let H be a group (not necessarily finite). A *character* of H is a group homomorphism $H \to E^*$.

Proposition 5.8 (Dedekind)**.** *Let $\chi_1, \ldots, \chi_k$ be distinct characters of H with values in E^*. Let $a_1, \ldots, a_k \in E$ and suppose that*

$$a_1\chi_1(h) + \cdots + a_k\chi_k(h) = 0$$

for all $h \in H$. Then $a_1 = a_2 = \cdots = a_k = 0$.

Proof. The proof is by induction on the parameter k. The conclusion of the proposition clearly holds if $k = 1$. Suppose that $k \geq 2$ and that the proposition holds for any strictly smaller parameter. If all the a_i vanish, there is nothing to prove, so we may assume that at least one a_i does not vanish. Up to reordering the indices, we may suppose wrog that it is a_2, ie we may suppose that $a_2 \neq 0$.

Pick $\alpha \in E$ such that $\chi_1(\alpha) \neq \chi_2(\alpha)$. For any $\beta \in E$, we have

$$\sum_{i=1}^{k} a_i\chi_i(\alpha\beta) = \sum_{i=1}^{k} a_i\chi_i(\alpha)\chi_i(\beta) = 0$$

and

$$\chi_1(\alpha)\sum_{i=1}^{k} a_i\chi_i(\beta) = \sum_{i=1}^{k} a_i\chi_1(\alpha)\chi_i(\beta) = 0.$$

Subtracting one expression from the other, we see that

$$\sum_{i=2}^{k} a_i(\chi_i(\alpha) - \chi_1(\alpha))\chi_i(\beta) = 0.$$

Since this holds for any $\beta \in E$, we conclude from the inductive hypothesis that $a_2 = 0$, a contradiction. □

Proof. (of Theorem 5.7). Let $\alpha \in L$. We compute

$$\sigma(\beta(\alpha)) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \cdots + \omega^{n-1}\alpha = \omega^{n-1}\beta(\alpha) = \omega^{-1}\beta(\alpha).$$

We deduce from this that for any integer i, we have

$$\sigma^i(\beta(\alpha)) = \omega^{-i}\beta(\alpha).$$

Furthermore, we then have

$$\sigma(\beta(\alpha)^n) = \sigma(\beta(\alpha))^n = \omega^{-n}\beta(\alpha)^n = \beta(\alpha)^n$$

and thus $\beta(\alpha)^n \in K$.

Now note that any element of $\mathrm{Gal}(L|K)$ defines a character on L^* with values in L^*. From Proposition 5.8, we conclude that there is $\alpha \in L^*$ st $\beta(\alpha) \neq 0$. Suppose that $\alpha \in L^*$ and that $\beta(\alpha) \neq 0$ from now on. Let $a := \beta^n$. Since the $\omega^{-i}\beta$ are all roots of $x^n - a$, we have shown that $x^n - a$ splits in L. Furthermore, we have shown above that $\mathrm{Gal}(L|K)$ acts faithfully and transitively on the roots of $x^n - a$. We conclude from Lemma 4.6 that $x^n - a$ is irreducible over K. Hence $[K(\beta) : K] = n = [L : K]$ (by Theorem 3.17 and the note after Proposition 3.9). We conclude from the tower law that $K(\beta) = L$. Thus L is a splitting field for $x^n - a$. □

END OF LECTURE 11

5.3 Radical extensions

5.3.1 Solvable groups

Definition 5.9. *Let G be a group. A finite filtration of G is finite ascending sequence $G_\bullet$ of subgroups $0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ such that G_i is normal in G_{i+1} for all $i \in \{0, \ldots, n-1\}$.*

The number n is called the length of the finite filtration.

The finite filtration $G_\bullet$ is said to have no redundancies if $G_i \neq G_{i+1}$ for all $i \in \{0, \ldots, n-1\}$.

The finite filtration $G_\bullet$ is said to have abelian quotients if the quotient group G_{i+1}/G_i is an abelian group for all $i \in \{0, \ldots, n-1\}$.

Finally, the finite filtration $G_\bullet$ is said to be trivial if $n = 1$.

Note that that (trivially...) the trivial filtration always exists and is unique.

Definition 5.10. *A group is said to be solvable if there exists a finite filtration with abelian quotients on G.*

Recall also that a group G is *simple* if it has no non trivial normal subgroups.

Lemma 5.11. *Let G be a solvable group and let H be a subgroup. Then H is solvable. If H is normal in G, then the quotient group G/H is also solvable.*

Proof. We shall write the group operation on G multiplicatively. Let $G_\bullet$ be a finite filtration with abelian quotients on G. Let n be the length of the filtration. Note that for all $i \in \{0, \ldots, n-1\}$, the group $H \cap G_i$ is normal in $H \cap G_{i+1}$. Indeed, for any $h \in H \cap G_{i+1}$, the automorphism $\gamma \mapsto h^{-1}\gamma h$ of G_{i+1} sends H into H and G_i into G_i, and thus sends $H \cap G_i$ into $H \cap G_i$. Thus $0 = G_0 \cap H \subseteq G_1 \cap H \subseteq \cdots \subseteq G_n \cap H = H$ is a finite filtration of H. Furthermore, for all $i \in \{0, \ldots, n-1\}$ there is an injective map of groups

$$\phi : G_{i+1} \cap H / G_i \cap H \hookrightarrow G_{i+1}/G_i$$

such that for all $\gamma \in G_{i+1} \cap H$, $\phi([\gamma]_{G_i \cap H}) = [\gamma]_{G_i}$. Hence $G_{i+1} \cap H / G_i \cap H$ is abelian. We have thus exhibited a finite filtration with abelian quotients for H. Hence H is solvable.

For the second statement, consider the ascending sequence of subgroups

$$0 = [G_0]_H \subseteq [G_1]_H \subseteq \cdots \subseteq [G_n]_H = G/H$$

of G/H. Let $i \in \{0, \ldots, n-1\}$. Let $\gamma \in G_{i+1}$ and let $\tau \in G_i$. Using the fact that the map $[\bullet]_H : G \to G/H$ is a map of groups, we compute

$$[\gamma]_H^{-1}[\tau]_H[\gamma]_H = [\gamma^{-1}\tau\gamma]_H.$$

Since $\gamma^{-1}\tau\gamma \in G_i$ because G_i is normal in G_{i+1}, we conclude that $[\gamma]_H^{-1}[\tau]_H[\gamma]_H \in [G_i]_H$. Since i, γ and τ were arbitrary, we conclude that the ascending sequence $[G_\bullet]_H$ is a finite filtration of G/H. Notice furthermore that there is a surjection of groups

$$\mu : G_{i+1}/G_i \to [G_{i+1}]_H/[G_i]_H$$

such that for any $\gamma \in G_{i+1}$, we have $\mu([\gamma]_{G_i}) = [[\gamma]_H]_{[G_i]_H}$. Since G_{i+1}/G_i is an abelian group by assumption, we see that $[G_{i+1}]_H/[G_i]_H$ is also abelian and thus $[G_\bullet]_H$ is a finite filtration with abelian quotients for G/H. $\square$

Lemma 5.12. *Let G be a group and let $H \subseteq G$ be a normal subgroup. Suppose that H is solvable and that G/H is solvable. Then G is solvable.*

Proof. Exercise. Construct a filtration with abelian quotients on G by glueing filtrations coming from G/H and H. $\square$

Proposition 5.13. *Let G be a finite group and let p be a prime number. Suppose that there is an $n \geq 0$ such that $\#G = p^n$. Then G is solvable.*

A finite group whose order is a power of a prime number p is a called a *p-group*.

Proof. By induction on n. The proposition clearly holds if $n = 0$. Let $\phi : G \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ be the map of groups such that $\phi(g)(h) = ghg^{-1}$ for any $g, h \in G$. This gives (by definition) an action of G on G (this is the "action by conjugation"). By the orbit-stabiliser theorem (see any first course on group theory) and Lagrange's theorem, the orbits of G in G all have cardinality a power of p. Note also that the orbit of the unit element 1_G of G is $\{1_G\}$ and thus has cardinality 1 (ie, it is a fixed point of the action). Since the orbits partition G, we see that there must be an element $g_0 \in G$ such that $g_0 \neq 1_G$ and such that g_0 is a fixed point of the action of G on G. By definition, g_0 commutes with every element of G, ie it belongs to the center $Z(G)$ of G (recall that the center of G is the subgroup of G consisting of the elements, which commute with all the elements of G). In particular, $Z(G) \neq \{1_G\}$. By definition, the group $Z(G)$ is abelian and thus solvable. Furthermore, the quotient group $G/Z(G)$ has cardinality p^k for some $k < n$ and is thus solvable by the inductive hypothesis. Hence, by Lemma 5.12, the group G is solvable. $\square$

Definition 5.14. *The length* $\mathrm{length}(G)$ *of a finite group G is the quantity*

$$\sup\{n \in \mathbb{N} \,|\, n \text{ is the length of a finite filtration with no redundancies of } G\}$$

Note that the length of a finite group is necessarily finite, because the length cannot be larger than $\#G$.

Lemma 5.15. *Suppose that G is a finite solvable group and let $G_\bullet$ be finite filtration with no redundancies of length* $\mathrm{length}(G)$ *on G. Then for all $i \in \{0, \ldots, \mathrm{length}(G) - 1\}$, the group G_{i+1}/G_i is a cyclic group of prime order.*

Proof. Let $n := \text{length}(G)$. By Lemma 5.11, the quotients G_{i+1}/G_i are abelian groups for all $i \in \{0, \dots, n-1\}$. Let $i_0 \in \{0, \dots, n-1\}$ and suppose that G_{i_0+1}/G_{i_0} is not of prime order. By the structure theorem for finitely generated abelian groups G_{i_0+1}/G_{i_0} is isomorphic to a finite direct sum of cyclic groups, each of which has order a power of a prime number (see Rings and Modules). So we conclude that G_{i_0+1}/G_{i+0} has a proper non trivial subgroup. Call such a subgroup H. Let $q(\bullet) = [\bullet]_{G_{i_0}} : G_{i_0} \to G_{i_0+1}/G_{i_0}$ be the quotient map. Consider now the ascending sequence of subgroups of G

$$0 = G_0 \subseteq G_1 \subseteq \dots G_{i_0} \subseteq q^{-1}(H) \subseteq G_{i_0+1} \subseteq \cdots \subseteq G_n = G \tag{4}$$

Then $G_{i_0} \neq q^{-1}(H)$ and $G_{i_0+1} \neq q^{-1}(H)$ by assumption. The group H is normal in G_{i_0+1}/G_{i_0} since G_{i_0+1}/G_{i_0} is abelian, and $q^{-1}(H)$ is the kernel of the composition of q with the quotient map

$$G_{i_0+1}/G_{i_0} \to (G_{i_0+1}/G_{i_0})/H.$$

Thus the group $q^{-1}(H)$ is normal in G_{i_0+1}. Furthermore, there is a natural injection of groups

$$q^{-1}(H)/G_{i_0} \hookrightarrow G_{i_0+1}/G_{i_0}$$

and a natural surjection of groups $G_{i_0+1}/G_{i_0} \to G_{i_0+1}/q^{-1}(H)$. Since G_{i_0+1}/G_{i_0} is abelian, we conclude that the ascending sequence (4) is a finite filtration with abelian quotients on G. Furthermore, it has length $n+1$ by construction. This contradicts the fact that n is maximal and thus G_{i_0+1}/G_{i_0} must be of prime order. □

Note. Suppose more generally that G is a finite group and that $G_\bullet$ be finite filtration with no redundancies of length length(G) on G. A similar argument shows that for all $i \in \{0, \dots, \text{length}(G) - 1\}$, G_{i+1}/G_i is a non zero simple group.

Examples.

- abelian groups are solvable (by definition);

- the group S_3 is solvable. The ascending sequence

$$0 \subseteq A_3 \subseteq S_3$$

is a finite filtration of S_3, with quotients $A_3/0 \simeq A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.

- the group S_4 is also solvable but the groups A_5 and S_5 are not solvable. The group A_5 is in fact simple and non abelian (and thus only has a trivial finite filtration). By Lemma 5.11, this implies that S_n is not solvable for all $n \geq 5$ (because S_5 is naturally a subgroup of S_n for all $n \geq 5$).

END OF LECTURE 12

5.3.2 Solvability by radicals

Let $L|K$ be a finite field extension.

Definition 5.16. *The extension $L|K$ is said to be radical if $L = K(\alpha_1, \dots, \alpha_k)$ and there are natural numbers $n_1, \dots, n_k$ such that $\alpha_1^{n_1} \in K$, $\alpha_2^{n_2} \in K(\alpha_1)$, $\alpha_3^{n_3} \in K(\alpha_1, \alpha_2)$, $\dots$, $\alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$.*

We see from the definition that if $L|K$ and $M|L$ are radical extensions, then $M|K$ is a radical extension.

Example. Kummer extensions are radical. This fact will play an essential role below.

Lemma 5.17. *Let $L|K$ be a radical extension and let $J|L$ be a finite extension, such that the composed extension $J|K$ is a Galois extension. Then there is a field L', which is intermediate between J and L, such that the extension $L'|K$ is Galois and radical.*

Proof. Suppose that $L = K(\alpha_1, \dots, \alpha_k)$ and that there are natural numbers $n_1, \dots, n_k$ such that $\alpha^{n_1} \in K$, $\alpha^{n_2} \in K(\alpha_1)$, $\alpha^{n_3} \in K(\alpha_1, \alpha_2)$, $\dots$, $\alpha^n \in K(\alpha_1, \dots, \alpha_{k-1})$ (this exists by assumption). Let

$$G := \mathrm{Gal}(J|K) = \{\sigma_1, \dots, \sigma_t\}.$$

Note that for any $i \in \{1, \dots, k\}$ and any $\sigma \in G$, we have

$$\sigma(\alpha_i^{n_i}) = \sigma(\alpha_i)^{n_i} \in \sigma(K(\alpha_1, \dots, \alpha_{i-1})) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_{i-1})).$$

We conclude that the extension

$$K(\alpha_1, \dots, \alpha_k, \sigma_1(\alpha_1), \dots, \sigma_1(\alpha_k), \sigma_2(\alpha_1), \dots, \sigma_2(\alpha_k), \dots, \sigma_t(\alpha_1), \dots, \sigma_t(\alpha_k)) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

is also a radical extension of K. Since

$$\sigma(K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k)) = K(\sigma(\mathrm{Orb}(\alpha_1)), \dots, \sigma(\mathrm{Orb}(\alpha_k))) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

for any $\sigma \in G$, we see that $K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))|K$ is a Galois extension (see the note before Corollary 4.5). We may thus let $L' := K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$. □

Theorem 5.18. *Suppose that* $\mathrm{char}(K) = 0$. *Let $L|K$ be a finite Galois extension.*

(a) *If* $\mathrm{Gal}(L|K)$ *is solvable then there exists a finite extension $M|L$ with the following properties.*

(1) The composed extension $M|K$ is Galois.

(2) There is a map of K-extensions $K(\mu_{[L:K]}) \hookrightarrow M$.

(3) M is generated by the images of L and $K(\mu_{[L:K]})$ in M.

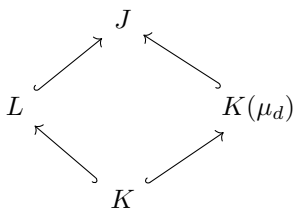
(4) The extension $M|K(\mu_{[L:K]})$ is a composition of Kummer extensions. In particular $M|K$ is a radical extension.

(b) *Conversely, if there exists a finite extension $M|L$ such that the composed extension $M|K$ is radical, then* $\mathrm{Gal}(L|K)$ *is solvable.*

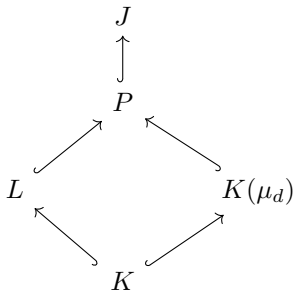
Note that the images of L and $K(\mu_c)$ in M do not depend on the maps of K-extensions $L \hookrightarrow M$ and $K(\mu_{[L:K]}) \hookrightarrow M$ (because $L|K$ and $K(\mu_{[L:K]})|K$ are Galois extensions; see Theorem 3.13 (iii)).

Proof. Let $d := \#\mathrm{Gal}(L|K) = [L : K]$. There exists a Galois extension of K and maps of K-extensions $K(\mu_d) \hookrightarrow J$ and $L \hookrightarrow J$. This follows from the existence of splitting extensions and Lemma 3.15. We choose such a Galois extension J and maps of K-extensions $K(\mu_d) \hookrightarrow J$ and $L \hookrightarrow J$.

By construction, we then have the following diagram of field extensions:



We let P be the field generated by L and $K(\mu_d)$ in J. This leads to the following diagram of field extensions:



Let $G := \mathrm{Gal}(J|K)$.

Now note the following.

(F1) $P|K$ is a Galois extension. Indeed, for all $\sigma \in G$, we have $\sigma(L) = L$ and $\sigma(K(\mu_d)) = K(\mu_d)$ (since L and $K(\mu_d)$ are Galois extensions of K) and thus $\sigma(P) = P$.

(F2) $P|K(\mu_d)$ is a Galois extension. This follows from the fact that $P|K$ is a Galois extension (see eg the note at the beginning of subsection 4.1).

(F3) The restriction map $\mathrm{Gal}(P|K(\mu_d)) \to \mathrm{Gal}(L|K)$ is injective. Indeed if $\sigma \in \mathrm{Gal}(P|K(\mu_d))$ restricts to Id_L on L, then σ fixes $K(\mu_d)$ and L. Thus σ must fix all of P, since P is generated by L and $K(\mu_d)$ over K.

We now prove (a). Suppose that $\mathrm{Gal}(L|K)$ is solvable. Then by (F3) and Lemma 5.11, we see that $\mathrm{Gal}(P|K(\mu_d))$ is solvable. In other words, there is a finite filtration with abelian quotients

$$0 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(P|K(\mu_d)).$$

By Lemma 5.15, we may assume that the quotients of this filtration are cyclic. Note that by the fundamental theorem of Galois theory 4.4, the subgroups H_i correspond to a decreasing sequence of subfields of P

$$P = P_n \supseteq P_{n-1} \supseteq \cdots \supseteq P_1 \supseteq P_0 = K(\mu_d)$$

such that $P_{i+1}|P_i$ is a Galois extension for any $i \in \{0, \ldots, n-1\}$. Furthermore, we then have

$$\mathrm{Gal}(P_{i+1}|P_i) \simeq H_{i+1}/H_i$$

so that $\mathrm{Gal}(P_{i+1}|P_i)$ is cyclic. Now note that by Lagrange's theorem, $\#(H_{i+1}/H_i)$ is a divisor of $\#\mathrm{Gal}(P|K(\mu_d))$, and thus of $\#\mathrm{Gal}(L|K) = d$ by (F3). Thus the polynomial $x^{\#\mathrm{Gal}(P_{i+1}|P_i)} - 1$ splits in $K(\mu_d)$. By Theorem 5.7, this implies that $P_{i+1}|P_i$ is a Kummer extension, and so in particular a radical extension. We conclude from this that $P|K(\mu_d)$ is a radical extension.

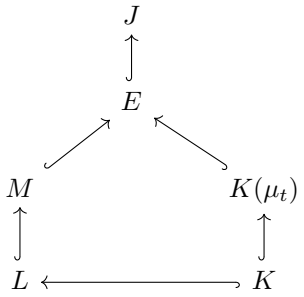
Now note that $K(\mu_d)|K$ is a radical extension, because $K(\mu_d)$ is generated over K by a generator ω of the group $\mu_d(K(\mu_d))$, and this generator satisfies the equation $\omega^d - 1 = 0$.

Thus $P|K$ is a radical extension.

Now set $M := P$. We have just seen that M satisfies (1), (2), (3) and (4), and we have thus completed the proof of (a).

We now prove (b). So suppose that there exists a finite extension $M|L$ so that the composed extension $M|K$ is a radical. So we may suppose that $M = K(\alpha_1, \ldots, \alpha_k)$ and that are natural numbers $n_1, \ldots, n_k$ such that

$\alpha_1^{n_1} \in K$, $\alpha_2^{n_2} \in K(\alpha_1)$, $\alpha_3^{n_3} \in K(\alpha_1, \alpha_2)$, $\dots$, $\alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$. Let $t := \prod_{i=1}^{k} n_i$. As before, choose a Galois extension $J|K$ such that there are maps of K-extensions $M \hookrightarrow J$ and $K(\mu_t) \hookrightarrow J$. Fix maps of K-extensions $M \hookrightarrow J$ and $K(\mu_t) \hookrightarrow J$. Let E be the field generated by M and $K(\mu_t)$ in J. We then have a diagram of extensions



Now we see from the definitions that $E = K(\mu_t)(\alpha_1, \dots, \alpha_k)$ and that

$$\alpha_1^{n_1} \in K(\mu_t),\ \alpha_2^{n_2} \in K(\mu_t)(\alpha_1),\ \alpha_3^{n_3} \in K(\mu_t)(\alpha_1, \alpha_2),\ \dots\ , \alpha_k^{n_k} \in K(\mu_t)(\alpha_1, \dots, \alpha_{k-1}).$$

Thus each of the extensions $K(\mu_t)(\alpha_1, \dots, \alpha_{i+1})|K(\mu_t)(\alpha_1, \dots, \alpha_i)$ is a Kummer extension, since $n_i|t$. Hence $\mathrm{Gal}(K(\mu_t)(\alpha_1, \dots, \alpha_{i+1})|K(\mu_t)(\alpha_1, \dots, \alpha_i))$ is an abelian group by Lemma 5.6. On the other hand, the group $\mathrm{Gal}(K(\mu_t)|K)$ is abelian by Proposition 5.4 (i) and Lemma 5.2. Applying Theorem 4.4 again, we conclude that $\mathrm{Gal}(E|K)$ is solvable. Now the group $\mathrm{Gal}(L|K)$ is a quotient of the group $\mathrm{Gal}(E|K)$ by Theorem 4.4 (iii) and is thus solvable by Lemma 5.11. □

The previous theorem motivates the following definition. Let $P(x) \in K[x]$ and let $L|K$ be a splitting extension for $P(x)$. We shall say that $P(x)$ is *solvable by radicals* if there is an extension $M|L$, such that the composed extension $M|K$ is radical (since all the splitting fields of $P(x)$ are isomorphic as K-extensions, this does not depend on the choice of a splitting field for $P(x)$). By the previous theorem, $P(x)$ is solvable by radicals iff the group $\mathrm{Gal}(L|K)$ is solvable.

Corollary 5.19. *Let $n \geq 5$ and let K is a field. The extension $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ is not radical.*

Here we consider the action of S_n on $K(x_1 \dots, x_n)$, which is the action induced by the action of S_n on $K[x_1 \dots, x_n]$ (note that any ring automorphism of a domain induces an automorphism of its field of fractions - this follows from Proposition-Definition 2.1). See before Theorem 2.16 for the definition of the action of S_n on $K[x_1 \dots, x_n]$.

Proof. Note that the extension $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ is a Galois extension by Artin's lemma. On the other hand, we saw at the end of subsubsection 5.3.1 that the group S_n is not solvable for $n \geq 5$. By Theorem 5.18 the extension $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ cannot be radical. □

Note. The extension $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ is the splitting field the polynomial

$$U_n(x) = x^n - s_1(x_1, \dots, x_n)x^{n-1} + s_2(x_1, \dots, x_n)x^{n-2} - \dots + (-1)^n s_n(x_1, \dots, x_n) \in K(x_1 \dots, x_n)^{S_n}[x].$$

Indeed, the elements $x_1, \dots, x_n \in K(x_1 \dots, x_n)$ are (all the) roots of $U_n(x)$ (see before Theorem 2.16). Furthermore, the elements $x_1, \dots, x_n$ generate $K(x_1 \dots, x_n)$ over K, and hence over $K(x_1 \dots, x_n)^{S_n}$. This gives another proof of the fact that $K(x_1 \dots, x_n)|K(x_1 \dots, x_n)^{S_n}$ is a Galois extension.

END OF LECTURE 13

5.3.3 The solution of the general cubical equation

We shall now illustrate Theorem 5.18 in a specific situation.

Let K be a field and suppose that $\mathrm{char}(K) = 0$. We wish to solve the cubical equation

$$y^3 + ay^2 + by + c = 0$$

where $a, b, c \in K$. Letting $x = y + \frac{a}{3}$, we obtain the equivalent equation

$$x^3 + px + q = 0 \tag{5}$$

where

$$p = -\frac{1}{3}a^2 + b$$

and

$$q = \frac{2}{27}a^3 - \frac{1}{3}ab + c.$$

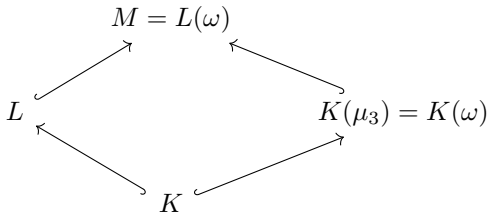
Let $P(x) := x^3 + px + q$. We want to find a formula for the roots of $P(x)$ of the following form. It should start with the elements $\{p, q\}$ and it should only involve iterations of the following operations:

- multiplication and addition;

- multiplication by elements of K;

- extraction of 2nd and 3rd roots (ie $\sqrt{\bullet}$ and $\sqrt[3]{\bullet}$).

Let $L|K$ be a splitting extension for $P(x)$. Let $\omega \in K(\mu_3)$ be a primitive 3rd root of unity. Now invoke Lemma 3.15 and the existence of splitting extensions to construct a finite Galois extension $J|K$ and maps of K-extensions $L \hookrightarrow J$ and $K(\mu_3) = K(\omega) \hookrightarrow J$. Let $M = L(\omega)$ be the field generated in J by the images of L and $K(\omega)$ in J. The situation is summarised by the following commutative diagram of field extensions



Note that such a diagram was considered in the proof of Theorem 5.18. Since $\mathrm{Gal}(L|K)$ is a solvable (because it can be realised as a subgroup of S_3), the argument given in the proof of Theorem 5.18 actually shows that $M|K$ is radical. The calculations below exploit (and reprove) precisely this fact.

Consider the sequence of extensions

$$K \hookrightarrow K(\omega) \hookrightarrow K(\omega, \sqrt{\Delta_P}) \hookrightarrow M$$

(note that by definition any square root of Δ_P is a polynomial in the roots of $P(x)$ and therefore lies in L).

Note that $[K(\omega) : K] \leq 2$ (by Proposition 5.4) and that $[K(\omega, \sqrt{\Delta_P}) : K(\omega)] \leq 2$ (by construction).

Note also that M is a splitting field of $P(x)$ over $K(\omega, \sqrt{\Delta_P})$ (by construction). Thus, using Lemma 4.7 (4), we see that $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ can be realised as a subgroup of $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. We conclude that either $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ is the trivial group or $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P})) \simeq \mathbb{Z}/3\mathbb{Z}$.

Let now $\alpha_1, \alpha_2, \alpha_3 \in L$ be the three roots of $P(x)$, with multiplicities. Let

$$\beta := \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \in M$$

and

$$\gamma := \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \in M.$$

Note that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

(because $-(\alpha_1 + \alpha_2 + \alpha_3)$ is the coefficient of x^2 in $P(x)$). In particular, we have

$$\alpha_1 := \frac{1}{3}(\beta + \gamma)$$

(because $1 + \omega + \omega^2 = 0$) and by a similar reasoning

$$\alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma)$$

and

$$\alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma).$$

Now we claim that β^3 and γ^3 lie in $K(\omega, \sqrt{\Delta_P})$. If $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P}))$ is the trivial group, then $M = K(\omega, \sqrt{\Delta_P})$ by Theorem 4.4 and then the claim holds tautologically. If $\mathrm{Gal}(M|K(\omega, \sqrt{\Delta_P})) \simeq \mathbb{Z}/3\mathbb{Z}$, then the claim follows from by Theorem 5.7 and Lemma 4.6 (note that in this case, $P(x)$ is irreducible and the roots have no multiplicities (why?)). So we see that the minimal polynomials of β^3 and γ^3 over $K(\omega)$ are of degree ≤ 2. In other words, β^3 and γ^3 satisfy quadratic equations with coefficients in $K(\omega)$. In turn, the elements of $K(\omega)$ satisfy quadratic equations with coefficients in K. We may thus express α_1, α_2 and α_3 by a formula involving only multiplications, additions and extractions of 2nd and 3rd roots. We make this explicit.

Using the fact that $1 + \omega + \omega^2 = 0$, we compute

$$\beta\gamma = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3.$$

Note also that

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2\alpha_1\alpha_2 + 2\alpha_1\alpha_3 + 2\alpha_2\alpha_3.$$

Thus

$$\beta\gamma = \beta\gamma - (\alpha_1 + \alpha_2 + \alpha_3)^2 = -3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p.$$

Similarly, we compute

$$\beta^3 + \gamma^3 = -27q = 27\alpha_1\alpha_2\alpha_3.$$

Thus β^3 and γ^3 are the roots of the quadratic equation

$$x^2 + 27qX - 27p^3 = 0.$$

Putting everything together, we see that the solutions of the equation

$$y^3 + ay^2 + by + c = 0$$

are

$$\beta_1 = \frac{1}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2 + 108p^3}} + \frac{1}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2 + 108p^3}} - \frac{1}{3}a$$

$$\beta_2 = \frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2+108p^3}} + \frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2+108p^3}} - \frac{1}{3}a$$

$$\beta_3 = \frac{\omega}{3}\sqrt[3]{-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2+108p^3}} + \frac{\omega^2}{3}\sqrt[3]{-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2+108p^3}} - \frac{1}{3}a$$

for some choices of 3rd roots of $-\frac{27}{2}q + \frac{1}{2}\sqrt{729q^2+108p^3}$ and $-\frac{27}{2}q - \frac{1}{2}\sqrt{729q^2+108p^3}$ (not all of them will give solutions). Here

$$p = -\frac{1}{3}a^2 + b$$

and

$$q = \frac{2}{27}a^3 - \frac{1}{3}ab + c.$$

Remark. The formulae above are actually valid more generally if $\mathrm{char}(K) \neq 2, 3$.

END OF LECTURE 14

6 Some group facts. Insolvable quintics.

Let G be a finite group.

Theorem 6.1 (Sylow). *Suppose that $\#G = p^n a$, where $(a,p) = 1$, p is prime and $n \geq 0$. Then there is a subgroup $H \subseteq G$ such that $\#H = p^n$. Furthermore, if $H, H' \subseteq G$ are two subgroups such that $\#H = \#H' = p^n$ then there exist a $g \in G$ such that $g^{-1}Hg = H'$.*

Proof. Omitted. See any second course on finite group theory. □

A subgroup $H \subseteq G$ as in the theorem is called a *p-Sylow subgroup* of G. According to the theorem, any two p-Sylow subgroups of G are conjugate.

Corollary 6.2 (Cauchy). *If p is prime and $p|\#G$, then there is an element of order p in G.*

Proof. Exercise. □

Let $n, k \geq 0$. Let $\sigma \in S_n$ and write $[\sigma]$ for the subgroup of σ generated by σ. Recall that σ is is said to be a *k-cycle*, if

- $[\sigma]$ has one orbit of cardinality k in $\{1, \ldots, n\}$;

- all the other orbits of $[\sigma]$ have cardinality 1.

Note that an orbit of cardinality 1 is a subset of $\{1, \ldots, n\}$ consisting of a fixed point of σ. Note also that a k-cycle necessarily has order k (why?). A transposition is none other than a 2-cycle.

Lemma 6.3. *Let p be a prime number and let $\sigma \in S_p$. Suppose that the order of σ is p. Then σ is a p-cycle.*

Proof. Let $a \in \{1, \dots, p\}$. By elementary group theory, we have $\#\mathrm{Orb}([\sigma], a) \cdot \#\mathrm{Stab}([\sigma], a) = p$. Since the only subgroups of $[\sigma]$ are $[\sigma]$ and the trivial group, we conclude that $\#\mathrm{Orb}([\sigma], a)$ is equal to either p or 1. Let A be the number of orbits with cardinality p and let B be the number of fixed points of σ. We then have $pA + B = p$ and thus $B = 0$ and $A = 1$, ie $[\sigma]$ has exactly one orbit, and it has cardinality p. In particular, σ is a p-cycle. □

Proposition 6.4. *Let p be a prime number. Let $\sigma, \tau \in S_p$ and suppose that σ is a transposition and that τ is a p-cycle. Then σ and τ generate S_p.*

Proof. Omitted. □

Proposition 6.5. *Let p be a prime number and let $P(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Suppose that $P(x)$ has precisely $p-2$ real roots in $\mathbb{C}$. Then $\mathrm{Gal}(P) \simeq S_p$.*

Proof. Let $L|\mathbb{Q}$ be a splitting field for $P(x)$. We identify L with the field generated over $\mathbb{Q}$ by the roots of $P(x)$ in $\mathbb{C}$ (see the remark after Theorem 3.13). The roots of $P(x)$ are distinct since $P(x)$ is separable (see Lemma 3.6). Choosing a labelling of the roots of $P(x)$ in L, we may view $\mathrm{Gal}(L|K)$ as a subgroup of S_p. Since $P(x)$ is irreducible, the ring $\mathbb{Q}[x]/(P(x))$ is a field and there is a map of $\mathbb{Q}$-extensions $\mathbb{Q}[x]/(P(x)) \hookrightarrow L$ and so $p|[L:K]$. Since $\#\mathrm{Gal}(L|K) = [L:K]$, we thus see that $p|\#\mathrm{Gal}(L|K)$. We can thus conclude from Cauchy's theorem that there is an element σ of order p in $\mathrm{Gal}(L|K)$. From Lemma 6.3, we conclude that σ is a p-cycle of S_p. On the other hand, note that complex conjugation is a field automorphism of $\mathbb{C}$. Since $L|\mathbb{Q}$ is a Galois extension, we see that the image of L under complex conjugation is again L (see Theorem 3.13 (iii)). Hence it restricts to an element κ of $\mathrm{Gal}(L|\mathbb{Q})$. We have $\kappa \neq \mathrm{Id}_L$, since $P(x)$ has non real roots by assumption. Let $\alpha, \beta \in L$ be the two non real roots of $P(x)$. Then we must have $\kappa(\alpha) = \beta$, since κ fixes all the other roots of $P(x)$ by assumption and $\kappa \neq \mathrm{Id}_L$. In particular, κ is a transposition in S_p. By Proposition 6.4, the elements κ and σ generated S_p and thus $\mathrm{Gal}(L|K) = S_p$. □

Corollary 6.6. *The polynomial $x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals.*

Proof. The polynomial $P(x) := x^5 - 6x + 3$ is irreducible by Eisenstein's criterion (for $p = 3$). Furthermore, we compute $P(-1) = 8 > 0$ and $P(1) = -2 < 0$. Also $\lim_{x\to\infty} P(x) = \infty$ and $\lim_{x\to-\infty} = -\infty$. Hence $P(x)$ has roots in $(-\infty, -1)$, $(-1, 1)$ and $(1, \infty)$ (by the intermediate value theorem). In particular, $P(x)$ has at least three roots in $\mathbb{R}$. Furthermore, we compute

$$\frac{\mathrm{d}}{\mathrm{d}x} P(x) = 5x^4 - 6$$

and the real roots of $\frac{\mathrm{d}}{\mathrm{d}x} P(x)$ are $\pm\sqrt[4]{\frac{6}{5}}$. If $P(x)$ had more than three roots in $\mathbb{R}$, the polynomial $\frac{\mathrm{d}}{\mathrm{d}x} P(x)$ would have at least three roots in $\mathbb{R}$ by the mean value theorem, which is not possible. We conclude that $P(x)$ has precisely $3 = 5 - 2$ roots in $\mathbb{R}$. We can thus conclude from Proposition 6.5 that $\mathrm{Gal}(P) \simeq S_5$. Since S_5 is not solvable (see the end of subsubsection 5.3.1), we conclude from Theorem 5.18 that $P(x)$ is not solvable by radicals. □

END OF LECTURE 15

7 The fundamental theorem of algebra via Galois theory

We will now prove that $\mathbb{C}$ is algebraically closed using Galois theory and basic real analysis. We shall need the following well-known fact.

Lemma 7.1. *Let $P(x) \in \mathbb{R}[x]$ be a monic polynomial of odd degree. Then $P(x)$ has a root in $\mathbb{R}$.*

Proof. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. When $x \neq 0$, we have

$$P(x) = x^n(1 + a_{n-1}/x + a_{n-2}/x^2 + \cdots + a_0/x^n).$$

Since

$$\lim_{x \to \pm\infty} 1 + a_{n-1}/x + a_{n-2}/x^2 + \cdots + a_0/x^n) = 1$$

there is a real number $x_1 > 0$ such that $1 + a_{n-1}/x_1 + a_{n-2}/x_1^2 + \cdots + a_0/x_1^n > 0$. Similarly, there is a real number $x_1 < 0$ such that $1 + a_{n-1}/x_0 + a_{n-2}/x_0^2 + \cdots + a_0/x_0^n > 0$. On the other hand, $x_0^n < 0$ and $x_1^n > 0$, so $P(x_0) < 0$ and $P(x_1) > 0$. We conclude from the intermediate value theorem that $P(x)$ has a root in the interval $[x_0, x_1]$. $\square$

Theorem 7.2. *The field $\mathbb{C}$ is algebraically closed.*

In the following, if

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$$

we shall write $\bar{P}(x)$ for the polynomial

$$P(x) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0 \in \mathbb{C}[x]$$

(where $(\bullet)$ is complex conjugation). Note that if $Q(x) = P(x)\bar{P}(x)$, then $\bar{Q}(x) = Q(x)$, so that $Q(x) \in \mathbb{R}[x]$ (check).

Proof. Let $P(x) \in \mathbb{C}[x]$. We need to show that $P(x)$ splits. Replacing $P(x)$ by $P(x)\bar{P}(x)$, we may even assume that the degree of $P(x)$ is even and has coefficients in $\mathbb{R}$.

Let $L|\mathbb{R}$ be a splitting field of $P(x)$. Let $G := \mathrm{Gal}(L|\mathbb{R})$. Let $G_2 \subseteq G$ be a 2-Sylow subgroup of G. Let $M = \mathbb{C}^{G_2}$. Then $[M : \mathbb{R}]$ is odd by the definition of Sylow subgroups and Theorem 4.4. Suppose that $M|\mathbb{R}$ is a non trivial extension and let $\alpha \in M \backslash \mathbb{R}$. Let $m_\alpha(x) \in \mathbb{R}[x]$ be the minimal polynomial of α. Then $\deg(m_\alpha(x))|[M : \mathbb{R}]$ by the tower law. In particular $\deg(m_\alpha(x))$ is odd. Thus, by Lemma 7.1, $m_\alpha(x)$ has a root in $\mathbb{R}$. Since $m_\alpha(x)$ is irreducible, this means that $\deg(m_\alpha(x)) = 1$. This contradicts the fact that $\alpha \in M \backslash \mathbb{R}$. We conclude that $M|\mathbb{R}$ is the trivial extension. In other words $G_2 = G$. In particular $\#G = 2^k$ for some $k \geq 0$. We may suppose wrog that $k > 0$ (otherwise $P(x)$ splits in $\mathbb{R}$ and there is nothing to prove).

Now by Proposition 5.13, the group is solvable. Thus, by Lemma 5.15, there is a filtration on G, which has cyclic quotients of order 2. As in the proof of Theorem 5.18, this gives rise via Theorem 4.4 to a sequence of subfields

$$L = L_n \supseteq L_{n-1} \supseteq \cdots \supseteq L_0 = \mathbb{R}$$

such that L_{i+1} is Galois over L_i for all $i \in \{0, \ldots, n-1\}$, and $\mathrm{Gal}(L_{i+1}|L_i) \simeq \mathbb{Z}/2\mathbb{Z}$. By Theorem 5.7, there exists $\beta \in L_1$ such that $\beta^2 \in L_0 = \mathbb{R}$ and such that $L_1 = \mathbb{R}(\beta)$. Since any positive element of $\mathbb{R}$ has

a square root in $\mathbb{R}$, we see that $\beta^2 < 0$ (because $L_1|L_0$ is a non trivial extension by assumption). Now we may compute

$$(\beta/\sqrt{|\beta^2|})^2 = \beta^2/|\beta^2| = -1.$$

Thus the polynomial $x^2+1 \in \mathbb{R}[x]$ has a root in L_1. In particular, x^2+1 splits in L_1. Since x^2+1 has no roots in $\mathbb{R}$ and $[L_1 : L] = 2$, we conclude that L_1 is a splitting field for x^2+1. In other words $L_1 \simeq \mathbb{C}$ as a $\mathbb{R}$-extension.

Now suppose that $k > 1$. By a similar reasoning, there is a $\rho \in L_2$, such that $\rho^2 \in L_1 \simeq \mathbb{C}$ and such that $L_2 = L_1(\rho)$. Furthermore $L_2|L_1$ is a non trivial extension by assumption. This is a contradiction, because any element of $L_1 \simeq \mathbb{C}$ has a square root (if $z = re^{i\theta}$, then $\sqrt{r}e^{i\theta/2}$ is a square root of z).

We conclude that $k = 1$ and thus $L = L_1 \simeq \mathbb{C}$. In particular, $P(x)$ splits in $\mathbb{C}$. $\square$

END OF LECTURE 16