Math 542

Instructor: Chenxi Wu

Email: cwu367@wisc.edu

Office Hours: TuWed 1-2pm Van Vleck 517, or by appointment

13.6

Definition. The **n-th cyclotomic polynomial** is the monic polynomial

$$\Phi_n(x) = \prod_{1\le j<n, \gcd(j,n)=1} (x - e^{\frac{2j\pi}{n}})$$

Theorem. $\Phi_n(x) \in \mathbb{Z}[x]$

Proof. By induction. $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Suppose $\Phi_k(x) \in \mathbb{Z}[x]$ for all k,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{1\le d<n, d|n} \Phi_d(x)}$$

which by long division of monic polynomials is in $\mathbb{Z}[x]$. □

Theorem. Φ_n are irreducible in $\mathbb{Q}[x]$ (hence also in $\mathbb{Z}[x]$).

Proof. Let $1 \le j < n$ such that $\gcd(j, n) = 1$, $\zeta = e^{\frac{2j\pi i}{n}}$, p prime and $p \not| n$. Let $f(x)$ be the minimal polynomial of ζ on $\mathbb{Q}$, and $\Phi_n(x) = f(x)g(x)$, and ζ^p is either a root of f or a root of g. f and g are both in $\mathbb{Z}[x]$ due to Gauss's Lemma.

- Firstly we show that ζ^p can not be a root of g.
  - If so, there is $h \in \mathbb{Z}[x]$ such that $g(x^p) = f(x)h(x)$ (Gauss's Lemma).
  - Pass to $\mathbb{F}_p$, we get

    $$(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$$

    Hence $q(x) = \gcd(\bar{f}(x), \bar{g}(x))$ has degree > 0.
  - This implies that $\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$ has a $(q(x))^2$ factor, which implies that $x^n - 1$ has a $(q(x))^2$ factor. This contradicts with the fact that $\gcd(x^n - 1, nx^{n-1}) = 1$ in $\mathbb{F}_p[x]$.
- Let f be the minimal polynomial of $e^{\frac{2\pi i}{n}}$. For any $1 \le j < n$ such that $\gcd(j, n) = 1$, $j = \prod_k p_k$ where p_k are primes that don't divide n. Repeatedly use the first step one gets $e^{\frac{2j\pi i}{n}}$ is also a root of f, hence $f = \Phi_n$.

□

Remark. As a consequence, $[\mathbb{Q}[e^{\frac{2\pi i}{n}}] : \mathbb{Q}] = \varphi(n)$.

14.1

Definition. Let K be a field, F a subfield.

- $Aut(K)$ is the set of automorphisms (isomorphisms from K to itself) of K.
- $Aut(K/F)$ is the set of automorphisms of K which when restricted to F is identity.

Example. We can calculate $Aut(\mathbb{C}/\mathbb{R})$: for any $\sigma \in Aut(\mathbb{C}/\mathbb{R})$, $\sigma(a+bi)$ (where $a, b \in \mathbb{R}$) equals $a + b\sigma(i)$, and

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

, Hence $\sigma(i) = \pm i$, σ is either $z \mapsto z$ or $z \mapsto \bar{z}$.

The following properties are obvious:

Theorem.
- $Aut(K)$ and $Aut(K/F)$ are groups under composition.
- $Aut(K/F)$ is a subgroup of $Aut(K)$.
- Any element in $Aut(K)$ preserves the prime field ($\mathbb{F}_p$ or $\mathbb{Q}$) k contained in K. In other words $Aut(K) = Aut(K/k)$.

□

The argument we used in the example above can be summarized as:

Theorem.
- If $\alpha \in K$ be the root of a polynomial $f(x) \in F[x]$, then so is $\sigma(\alpha)$ for any $\sigma \in Aut(K/F)$.
- If $K = F(\alpha)$, then $\sigma \in Aut(K/F)$ is uniquely determined by $\sigma(\alpha)$.

□

Furthermore we have:

Theorem. If $K = F(a)$, $[K : F] < \infty$, there is a bijection from $Aut(K/F)$ to the roots of the minimal polynomial of a in K.

Proof. The previous theorem implies that this map is well defined and injective. We only need to show surjectivity. Suppose a' is a root of the minimal polynomial $f(x)$ of a, then $K \cong F[x]/(f)$ and we identify the two by sending a to x. Now define a map $\sigma' : K[x] \to K$ by sending x to a', then

$$\ker(\sigma') = \{g \in F[x] : g(a') = 0\} \supseteq (f)$$

Hence σ' induces a homomorphism from K to K, which is identity when restricted to F and sends a to a'. Because K is a field it must be injective, and because K is a finite dimensional F-vector space it must be bijective. □

As a consequence we have:

Example.
- $Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, (\sqrt{3} \mapsto -\sqrt{3})\}$
- $Aut(\mathbb{Q}(3^{1/3})/\mathbb{Q}) = \{id\}$
- $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. Suppose α is the root of $x^3 + x + 1$, then so is α^2 and $\alpha^4 = \alpha^2 + \alpha$, hence $Aut(\mathbb{F}_8/\mathbb{F}_2)$ is a cyclic group of order 3.
- $Aut(\mathbb{C}(x)/\mathbb{C}) = \{x \mapsto \frac{ax+b}{cx+d} : ad - bc \neq 0\} \cong PSL(2, \mathbb{C})$
- Let K be the splitting field of $x^3 - 2$ on $\mathbb{Q}$, then $Aut(K/\mathbb{Q}) \cong S_3$, the isomorphism can be obtained via permuting the three roots of $x^3 - 2$.

Definition. Let $S \subset Aut(K/F)$, the **fixed field** is

$$K^S = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in S\}$$

It is easy to check that:

Theorem.
- K^S is a subfield of K.
- If $S \subseteq S'$, then $K^{S'} \subseteq K^S$.
- If $F \subseteq K_1 \subseteq K_2 \subseteq K$ is a sequence of subfields, then $Aut(K/K_2) \subseteq Aut(K/K_1)$.
- $F \subseteq K^{Aut(K/F)}$
- $Aut(K/K^S) \supseteq \langle S \rangle$

□

Definition. Let K/F be a finite extension. If $K^{Aut(K/F)} = F$, we call K/F a **Galois extension**, and $Aut(K/F)$ the **Galois group**.

14.2

A key theorem for automorphism group of finite extension is the following:

Theorem. If $G \subseteq Aut(K)$ is a finite subgroup, then $[K : K^G] = |G|$.

Proof. Suppose $[K : K^G] < |G|$. Let $G = \{\sigma_1, \ldots, \sigma_n\}$, then these n elements are K-linearly dependent as functions from K to K. Without loss of generality suppose $\sigma_1, \ldots, \sigma_k$ are K-linearly independent and $\sigma_{k+1} = \sum_{i=1}^{k} c_i \sigma_i(x)$, where $c_i \in K$. Then for any $x, y \in K$

$$\sum_{i=1}^{k} c_i \sigma_i(x)\sigma_i(y) = \sigma_{k+1}(xy) = \sigma(x)\sigma(y) = \sum_{i=1}^{k}\sum_{j=1}^{k} c_i c_j \sigma_i(x)\sigma_j(y)$$

Hence for all $1 \leq i \leq k$,

$$c_i \sigma_i(x) = \sum_{j=1}^{k} c_i c_j \sigma_j(x)$$

which implies that at most one c_i is non-zero, and the non-zero one must be 1, a contradiction.

Suppose $[K : K^G] > |G|$. Let $G = \{\sigma_1, \ldots, \sigma_n\}$, then there must be $n+1$ K^G-linearly independent elements in K, denote them as $x_1, \ldots, x_{n+1}$. Consider the vectors $v_i = \begin{bmatrix} \sigma_1(x_i) \\ \ldots \\ \sigma_n(x_i) \end{bmatrix} \in K^n$, these $n+1$ vectors must be K-linearly dependent. Without loss of generality, suppose $v_1, \ldots, v_k$ are K-linearly independent, and $v_{k+1} = \sum_{i=1}^{k} c_i v_i$. Then c_i can not all be in K^G due to the fact that $v_1, \ldots, v_{n+1}$ are K^G-linearly independent. Suppose $\sigma \in G$ such that $\sigma(c_1) \neq c_1$, then $v_{k+1} = \sum_{i=1}^{k} \sigma(c_i) v_i$, hence

$$\sum_{i=1}^{k} (c_i - \sigma(c_i)) v_i = 0$$

a contradiction. □

Remark. The first part of the proof above also showed that if $[K : F] < \infty$ then $|Aut(K/F)| \leq [K : F]$, and the elements of $Aut(K/F)$ must be K-linearly independent.

Remark. The theorem above implies that When $[K : F] < \infty$, K/F is Galois iff $|Aut(K/F)| = [K : F]$.

Example.

- $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ is not Galois, $\mathbb{Q}(2^{1/4})^{Aut(\mathbb{Q}(2^{1/4})/\mathbb{Q})} = \mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(2^{1/4})/\mathbb{Q}(\sqrt{2})$ is Galois.
- Cyclotomic extensions over $\mathbb{Q}$ are all Galois.
- $((\mathbb{F}_2(x))[y]/(y^2 - x))/(\mathbb{F}_2(x))$ is not Galois.

Theorem. A finite extension K/F is Galois iff it is the splitting field of some separable (i.e. $\gcd(f, f') = 1$) polynomial.

Proof. $\Longleftarrow$: Suppose $f(x) \in F[x]$, without loss of generality assume that it has no roots in F. If α is a root of f, let $p(x)$ be the minimal polynomial of α in F, which has d roots $\alpha_1 = \alpha, \ldots, \alpha_d$. By extensions of isomorphisms of splitting fields, $Aut(K/F)$ acts on $\{\alpha_1, \ldots, \alpha_d\}$ transitively, hence $|Aut(K/F)| = d|Aut(K/F(\alpha))|$, which because p is separable, equals $[F(\alpha) : F]|Aut(K/F(\alpha))|$. Induction on $[K : F]$ one gets the conclusion.

$\Longrightarrow$: Let $\{w_i\}_{i=1,\ldots,[K:F]}$ be a F-basis of K, consider the set $S = \{\sigma(w_i) : \sigma \in Gal(K/F), 1 \leq i \leq [K : F]\}$, and $f = \prod_{s \in S}(x - s)$. f is evidently separable as it has all roots with multiplicity 1, and coefficients of f are symmetric functions on the elements of S, and by construction any element in the Galois group permutes elements of S hence won't change f, hence $f \in F[x]$. □

Remark. The theorem above implies that if K/F is a finite Galois extension, E is a subfield of K that contains F, then K/E is also a Galois extension.

Theorem. (Theorem 14 in Dummit & Foote, Fundamental Theorem of Galois Theory) Let K/F be a finite Galois extension with Galois group $G = Gal(K/F)$. There is a bijection from the set of subgroups of $Gal(K/F)$ and subfields of K that contains F defined by $H \leq G \mapsto K^H \subseteq K$, $E \subseteq K \mapsto Aut(K/E) < G$, such that if $E = K^H$, $E' = K^{H'}$ then

1. $H \leq H'$ iff $E' \subseteq E$.
2. $[K : E] = |H|$, $[E : F] = |G/H|$.
3. K/E is always Galois, $Gal(K/E) = H$.
4. E/F is Galois iff H is a normal subgroup of G, in which case $Gal(E/F) \cong G/H$. In general, embeddings of E into K that preserves F are in 1-1 correspondence with cosets of H in G.
5. $E \cap E' = K^{\langle H, H' \rangle}$.

Proof.
- Firstly show bijection. It is evident that for any $H \leq G$, $H \leq Aut(K/K^H)$. However $|Aut(K/K^H)| \leq [K : K^H] = |H|$, hence they are equal. On the other hand, if E is a subfield of K that contains F, then K/E is Galois, hence $E = K^{Aut(K/E)}$.
- 1, 5 are obvious, 2, 3 follows from the fact that K/E is Galois. For 4, consider the G-action on the set of embeddings of E into K by $\sigma \cdot i = \sigma \circ i$. The fact that this action is transitive is due to the extension of isomorphisms of splitting fields, and 4 follows.

□

Midterm 2 Review

Topics covered:

- Splitting fields (13.4)
- Separability (13.5)
- Cyclotomic polynomial (13.6)

Practice problems:

- Let $F = \mathbb{F}_p$, p prime number, K be the splitting field of $x^6 - 1$. What is $[K : F]$?
- Let $F = \mathbb{F}_3(t)$, $f \in F[x]$ monic with degree 3, K the splitting field of f. Find f such that $[K : F] = 1, 2, 3, 6$.
- Let F be a field of characteristic p, K/F a finite extension. Show that if $p \not| [K : F]$ then K/F is separable.

14.7

Galois group of generic polynomials

Definition. Let k be a field, a polynomial in $k[x_1, \ldots, x_n]$ is called **symmetric** if it is invariant under permutation of x_i. The **elementary symmetric polynomials** $e_1, \ldots, e_n$ are defined by

$$\prod_i (x - x_i) = \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} x^i$$

In other words,

$$e_i(x_1, \ldots, x_n) = \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} \prod_{k=1}^{i} x_{j_k}$$

Theorem. (Fundamental Theorem of symmetric polynomial) Let k be a field, then any symmetric polynomial over k can be uniquely written as a polynomial of the elementary symmetric polynomials. In other words, the sub-ring of symmetric polynomials in $k[x_1, \ldots, x_n]$ is isomorphic to polynomial ring $k[t_1, \ldots, t_n]$ by $t_i \mapsto e_i$.

Remark. A common proof is via Noether normalization lemma. Another proof is outlined in the exercises of Dummit & Foote.

Proof. Define a linear order $<_1$ on $\mathbb{N}^n$ (seen as set of degrees of a monomial $a_{d_1,\ldots,d_n} x_1^{d_1} \ldots x_n^{d_n}$) as:

$$(d_1, \ldots, d_n) <_1 (d'_1, \ldots, d'_n)$$

iff

$$d_i < d'_i \text{ and } d_j = d'_j \text{ for all } j < i$$

another linear order $<_2$ such that

$$(d_1, \ldots, d_n) <_2 (d'_1, \ldots, d'_n)$$

iff

$$(d_1 + \cdots + d_n, d_2 + \cdots + d_n \ldots, d_n) <_1 (d'_1 + \cdots + d'_n, d'_2 + \cdots + d'_n, \ldots, d'_n)$$

Then one can verify the following:

1. If f is a symmetric polynomial in $k[x_1, \ldots, x_n]$, then the leading non-zero term under $<_1$ is of the form $a_{d_1,\ldots,d_n} x_1^{d_1} \ldots x_n^{d_n}$ where $d_1 \ge d_2 \ge \cdots \ge d_n$.
2. If f, g are in $k[x_1, \ldots, x_n]$, the leading non-zero term (under $<_1$) of fg is the product of the leading non-zero terms of f and of g.

3. It follows from statement 2. above, that the leading non-zero term of $e_1^{d_1} \dots e_n^{d_n}$ under $<_1$ is

$$x_1^{d_1+\dots+d_n} x_2^{d_2+\dots+d_n} \dots x_n^{d_n}$$

4. Statement 3. above implies that if the leading term of g under $<_2$ is $b_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$, then the leading term of $g(e_1, \dots, e_n)$ under $<_1$ is

$$b_{i_1,\dots,i_n} x_1^{i_1+\dots+i_n} x_2^{i_2+\dots+i_n} \dots x_n^{i_n}$$

Now given any symmetric polynomial f, statement 1 above implies that the leading term of f under $<_1$ is of the form

$$f_{d_1,\dots,d_n} x_1^{d_1} \dots x_n^{d_n}$$

and $d_1 \geq d_2 \geq \dots d_n$. Statement 3 above implies that the leading term of

$$f - f_{d_1,\dots,d_n} e_1^{d_1-d_2} e_2^{d_2-d_3} \dots e_n^{d_n}$$

under $<_1$ is lower than the leading term of f. Because there are only finitely many n-tuples $(d_1, \dots, d_n)$ that satisfy $d_1 \geq \dots \geq d_n$ smaller than any element in $\mathbb{N}^n$ under $<_1$, repeating the procedure one would eventually terminate, hence f can be written as $g(e_1, \dots, e_n)$ where g is a polynomial.

On the other hand, statement 4 above implies that the leading coefficient of g under $<_2$ must be identical to the leading coefficient of f under $<_1$. Let this leading term of g be m, then carry out the same argument on $f - m(e_1, \dots, e_n)$ and $g - m$, we can show that all coefficients of g are uniquely determiened by coefficients of f, hence the uniqueness. □

Example. The proof above provides an algorithm to write a symmetric polynomial as polynomials of $e_1, \dots, e_n$. For example, when $n = 3$, $f = x_1^3 + x_2^3 + x_3^3$. Leading term under $<_1$ is x_1^3, hence subtract by $1 \cdot e_1^{3-0} e_2^{0-0} e_3^0 = e_1^3$, we get

$$f - e_1^3 = -3x_1^2 x_2 - 3x_1^2 x_3 - 3x_2^2 x_1 - 3x_2^2 x_3 - 3x_3^2 x_1 - 3x_3^2 x_2 - 6x_1 x_2 x_3$$

Now leading term is $-3x_1^2 x_2$, subtract by $-3 \cdot e_1^{2-1} e_2^{1-0} e_3^0 = -3e_1 e_2$, we get

$$f - e_1^3 + 3e_1 e_2 = 3x_1 x_2 x_3$$

So

$$f = e_1^3 - 3e_1 e_2 + 3e_3$$

An immediate consequence is the following:

Theorem. Let k be a field, $F = k(t_1, \dots, t_n)$, K the splitting field of $x^n + t_1 x^{n-1} + \dots + t_n$, then $Gal(K/F) = S_n$.

□

Nested Roots and Solvable extension

Theorem. If F is characteristic 0 and has all primitive n-th root of unity (e.g. $F = \mathbb{C}(t_1, \ldots, t_n)$), K is the splitting field of irreducible polynomial $x^n - a \in F[x]$, then $Gal(K/F) \cong \mathbb{Z}/n$.

Proof. Let α be a root of $x^n - a$ in K, ζ be a primitive root of 1, then the roots of $x^n - a$ are $\zeta^k \alpha$, where $0 \leq k < n$, and Galois group elements are $\sigma_k(\alpha) = \zeta^k \alpha$ where $0 \leq k < n$. It is easy to see that this group is isomorphic to $\mathbb{Z}/n$. □

Theorem. If F is char 0 and has all primitive roots of unity. K/F a finite Galois extension, L splitting field of irreducible polynomial $x^n - a \in K[x]$, then there is a finite extension L'/K, such that $L \subseteq L'$, L'/F is Galois, and $Gal(L'/K)$ is abelian.

Proof. Let $g \in F[x]$ such that K is the splitting field of g, let $A = \{\sigma(a)\}$ be the orbit of a under $Gal(K/F)$, then $\prod_{a' \in A}(x^n - a')g(x) \in F[x]$, let L' be its splitting field over F, then $L \subseteq L'$.

For any $a' \in A$, let $\alpha_{a'}$ be a root of $x^n - a'$ in L', then any element of $Gal(L'/K)$ sends $\alpha_{a'}$ to some $\zeta_{a'}^k \alpha_{a'}$, here $\zeta \in F$ is a primitive n-th root of unity. This gives an injection from $Gal(L'/K)$ to $(\mathbb{Z}/n)^{|A|}$, hence $Gal(L'/K)$ is abelian. □

Definition. A group G is called **solvable** if there is a finite sequence of nested subgroups

$$0 = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G$$

Such that G_{k+1} is normal in G_k and G_k/G_{k+1} are all abelian.

Remark. Solvability is closed under subgroups, quotients and extensions. As a consequence, if α can be written down using arithmetic operations, elements in F as well as nested k-th roots, (more precisely, if α is an element in a finite extension which is a finite composition of extensions of the form $(K[x]/(x^k - a))/K)$ then α lies in some finite Galois extension where the Galois group is solvable.

Example. The roots of $x^5 + t_1 x^4 + t_2 x^3 + t_3 x^2 + t_4 x + t_5$ can not be written using constants, t_i and taking successive roots. Because if otherwise, the splitting field of this polynomial over $\mathbb{C}(t_1, \ldots, t_5)$ will be a quotient of a solvable group hence solvable, and S_5 has a normal subgroup A_5 which is a finite simple group.

Cyclic extensions

Theorem. If F has characteristic 0, contains all primitive n-th roots of unity, K/F a Galois extension and $Gal(K/F)$ is a cyclic group of order n. Then K is the splitting field of a polynomial of the form $x^n - a$ where $a \in F$.

Proof. Let ζ be a primitive n-th root of unity in F, σ be a generator of $Gal(K/F)$. Because the elements of $Gal(K/F)$ are K-linearly independent, there is some $\alpha \in K$ such that the **Lagrange Resolvent**

$$(\alpha, \zeta) = \sum_{j=0}^{n-1} \zeta^j \sigma^j(\alpha) \neq 0$$

It is easy to see that

$$\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \zeta)$$

Hence

$$(\alpha, \zeta)^n \in F$$

Let $a = (\alpha, \zeta)^n$, then the splitting field of $x^n - a$ over F is $F((\alpha, \zeta))$. On the other hand, any non-identity element in $Gal(K/F)$ does not fix (α, ζ), hence $F((\alpha, \zeta)) = K$. □

Remark. It is evident that for any n-th root of unity ζ, $(\alpha, \zeta)^n \in F$. By linear algebra, α can be solved from the values of (α, ζ) where ζ goes through all n-th root of unity. This shows that if F has all roots of unity and $Gal(K/F)$ is solvable, then elements in K can be written using elements in F, arithmetic operations and successive k-th roots.

Final Review

- If K/F finite, then $|Aut(K/F)| \leq [K : F]$.
- Let G be a finite subgroup of $Aut(G)$, then $[K : K^G] = |G|$.
- Let K/F be a finite extension. The followings are equivalent:
  - $F = K^{Aut(K/F)}$
  - $|Aut(K/F)| = [K : F]$
  - K is the splitting field of some separable polynomial.

  and when any of these is true we say K/F a Galois extension, and call $Aut(K/F)$ the Galois group $Gal(K/F)$.
- Fundamental Theorem of Galois Theory

Practice Problems:

1. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois, calculate its Galois group, and show that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ has degree 4.

Answer: This is the splitting field of separable polynomial $(x^2 - 2)(x^2 - 3)$. The extension is of degree 4 because $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Any element in the Galois group permutes the two roots of $x^2 - 2$ and the

two roots of x^2-3, and is determined by its action on these 4 roots, hence $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})\mathbb{Z}/2\times\mathbb{Z}/2$. $\sqrt{2}+\sqrt{3}$ is not fixed by any non-zero element of the Galois group, hence can not lie in any intermediate fields between $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}$, hence its minimal polynomial must have degree 4.

2. Let p be an odd prime, K the splitting field of x^p-2, find $Gal(K/\mathbb{Q})$.

Answer: $K=\mathbb{Q}(e^{\frac{2\pi i}{p}},\sqrt[p]{2})$, and the minimal polynomial of $e^{\frac{2\pi i}{p}}$ and $\sqrt[p]{2}$ over $\mathbb{Q}$ have degrees $p-1$ and p respectively, hence $[K:\mathbb{Q}]\leq p(p-1)$. Because $K_1=\mathbb{Q}(e^{\frac{2\pi i}{p}})$ and $K_2=\mathbb{Q}(\sqrt[p]{2})$ are both subfields of K, $[K_1:\mathbb{Q}]=p-1$, $[K_2:\mathbb{Q}]=p$, both $p-1$ and p are factors of $[K:\mathbb{Q}]$, hence $[K:\mathbb{Q}]=p(p-1)$.

Let $z_k=e^{\frac{2\pi ik}{p}}\sqrt[p]{2}$, then $\{z_k:0\leq k<p\}$ are all the roots of x^p-2, and $K=\mathbb{Q}(z_0,z_1)$, hence an element in $Gal(K/\mathbb{Q})$ is uniquely determined by its action on z_0 and z_1. On the other hand, because $x^p-2\in\mathbb{Q}[x]$, σ has to send z_0 and z_1 to some z_i and z_j respectively, and $i\neq j$. Hence we can label the elements of $Gal(K/\mathbb{Q})$ by a tuple $(i,j)\in\mathbb{Z}/p\times\mathbb{Z}/p$, such that $i\neq j$, denoted as $\{\sigma_{i,j}\}$. By computation it is easy to see that the identity element is $\sigma_{0,1}$ and the multiplication operation is $\sigma_{i,j}\sigma_{i',j'}=\sigma_{i'(j-i)+i,i+j'(j-i)}$.

3. Let K be the splitting field of $(x^3-2)(x^3-3)$, find $Gal(K/\mathbb{Q})$.

Answer: By an argument similar to 2 above we get $[K:\mathbb{Q}]=18$. Let $z_k=e^{\frac{2\pi ki}{3}}\sqrt[3]{2}$, $z_k=e^{\frac{2\pi ki}{3}}\sqrt[3]{3}$, then any element of $Gal(K/\mathbb{Q})$ is uniquely determined by its action on the sets $Z=\{z_0,z_1,z_2\}$ and $W=\{w_0,w_1,w_2\}$, i.e. $Gal(K/\mathbb{Q})\subseteq S_Z\times S_W\subseteq S_{Z\cup W}$. There are $3!\times3!=36$ elements in $S_Z\times S_W$ however, but if we impose an extra restriction, that $\sigma(z_1)/\sigma(z_0)=\sigma(w_1)/\sigma(w_0)$, will cut this number down to 18. In conclusion, $Gal(K/\mathbb{Q})$ is isomorphic to a subgroup of $S_{Z\cup W}=S_6$ generated by $(z_1,z_2)(w_1,w_2)$, (z_0,z_1,z_2) and (w_0,w_1,w_2).

4. Show that if K/F and K'/F are two Galois extensions, and there is an isomorphism $f:K\to K'$ which is identity when restricted to F, then $Gal(K/F)\cong Gal(K'/F)$.

Answer: Define group homomorphism $Gal(K/F)\to Gal(K'/F)$ by $\sigma\mapsto f\sigma f^{-1}$, and group homomorphism $Gal(K'/F)\to Gal(K/F)$ by $\sigma\mapsto f^{-1}\sigma f$, then these two homomorphisms are inverses of one another hence are both isomorphisms.

5. Let $F=\mathbb{F}_2(t)$ where t is transcendental over $\mathbb{F}_2$. Let K be the splitting field of x^6+x^2+t over F. Find $Aut(K/F)$ and $K^{Aut(K/F)}$.

Answer: Firstly we find the splitting field of x^6+x^2+t. By Gauss's Lemma we can show that this is an irreducible polynomial (it doesn't have root in $\mathbb{F}_2[t]$ hence no factor of degree 1. If it has a factor of degree 2, there are a_i, $b_i\in\mathbb{F}_2[f]$ such that $(x^2+a_1x+a_0)(x^4+b_3x^3+b_2x^2+b_1x+b_0)=x^6+x^2+t$. Compare

coefficients one get $b_3 = a_1$, $b_2 = a_0 + a_1^2$, $b_1 = a_1^3$, so $a_1 b_0 + a_1^3 a_0 = 0$, and $a_0 b_0 = t$, that's not possible. Similarly it can not have degree 3 factor).

Let K_1 be F adjoining one root α of $x^6 + x^2 + t$, then $K_1 = \mathbb{F}_2(\alpha)$ and α is transcendental over $\mathbb{F}_2$. In K_1 we have $x^6 + x^2 + t = (x+\alpha)^2(x^2 + \alpha x + \alpha^2 + 1)^2$, so to get the splitting field we need to add a root of $x^2 + \alpha x + \alpha^2 + 1$, denoted as β. Now $K = F(\alpha, \beta)$, and the three roots of $x^6 + x^2 + t$ are $\alpha, \beta, \alpha + \beta$.

Elements of $Aut(K/F)$ are uniquely determined by their action on this set of 3 roots, so it is a subgroup of S_3. $Aut(K/K_1)$ is a subgroup of order 2, and we also know that there are elements of $Aut(K/F)$ that sends α to β or $\alpha + \alpha$, so $Aut(K/K_1) \cong S_3$.

$K^{Aut(K/F)} = F(\alpha\beta(\alpha + \beta))$.

6. Suppose K/F is a finite Galois extension. Show that so is $K(t)/F(t)$ and these two extensions have the same Galois group.

Answer: Let $g \in F[x]$ be a separable polynomial where K is its splitting field, then $K(t)/F(t)$ is also the splitting field of $g \in (F(t))[x]$, and g is separable in $(F(t))[x]$ due to long division and Euclid's algorithm for gcd.

Any element in $Gal(K/F)$ induces an element in $Gal(K(t)/F(t))$, by applying σ to all coefficients. On the other hand, any $\sigma' \in Gal(K(t)/F(t))$ has to send t to t and elements of K to other elements of K (because those are all the elements of $K(t)$ which are algebraic over F). This shows that σ' must be induced by some element in $Gal(K/F)$.

7. Write down a Galois extension K/F such that $Gal(K/F) \cong S_3 \times \mathbb{Z}/3$. Let $a \in K$, m_a be the minimal polynomial of a in $F[x]$, what are the possible degrees of m_a?

Answer: Let $F = \mathbb{C}(t_1, t_2)$ be the field of rational functions with 2 parameters. Let K be the splitting field of $(x^3 + x + t_1)(x^3 - t_2)$. Let K_1 be the splitting field of $x^3 + x + t_1$ and K_2 be the splitting field of $x^3 - t_2$, then both K_1/F and K_2/F are Galois, hence $Gal(K/K_1)$ and $Gal(K/K_2)$ are two normal subgroups of $Gal(K/F)$ whose product is the whole group (because $K_1 \cap K_2 = F$) and intersection is 1 (because K is the smallest subfield of K that contains both K_1 and K_2), hence $Gal(K/F)$ is the product of these two groups. By calculation and problem 6 above these two groups are $\mathbb{Z}/3$ and S_3 respectively.

The possible degrees of m_a are just the possible degrees of extensions K'/F where K' is a subfield of K, in other words possible indices of subgroups of $Gal(K/F)$. These are: 1, 2, 3, 6, 9 and 18.