MATH5725: Galois Theory (S2,2014)
Lecture 2

1. Last time we saw a key example of Galois theory - a biquadraic field and its subfields.
2. Today we build up some of the theory needed to generalise that example, focusing on the existence of a splitting field.

Before continuing here are the basic facts about polynomials which we will use:
1. A polynomial $f \in k[X]$ is irreducible if it can not be written as a product of polynomials of degree more than 0 but less than that of f.
2. If $f(X), g(X) \in k[X] \backslash 0$; there exists unique polynomials $q, r \in k[X]$ such that $f = gq + r$, with the degree of r less than or equal to that of g. (Proof idea: the set $\{f - qg \mid q \in k[X]\}$ has an element of minimal degree which gives r).
3. Every polynomial can be written as a product of powers of irreducible polynomials in an essentially unique way. I.e. $k[X]$ is a unique factorisation domain. (Idea: the key point is to show that if f is irreducible and $f \mid gh$ then $f \mid g$ or $f \mid h$ which follows by applying 2 to write $g = fq + r$, and $h = fq' + r$).
4. The greatest common divisor of two polynomials is unique, up to multiplication by an element of k^*, and can be written as $\lambda g + \mu f$ (This is just the Euclidean algorithm, which holds because of 2).
5. If a polynomial $f(X) \in k[X]$ is irreducible then the ideal generated by it is maximal. This is because the gcd of an irreducible f polynomial and other polynomial g is 1 or f and the gcd of f and g is contained in the ideal (f, g).
E.g. $X^2 - 4$ is not irreducible as $X^2 - 4 = (X - 2)(X + 2)$. On the other hand $(X^2 - 2)$ is irreducible over $\mathbf{Q}$, for if it were not then

$$X^2 - 2 = (X - a)(X - b)$$

and with $a, b \in \mathbf{Q}$ and so $a^2 = 2$. But $\sqrt{2} \notin \mathbf{Q}$.

An important consequence of the above is that if K/k is algebraic and $\alpha \in K$ and $p(X) \in k[X]$ is then one can always "rationalise" the denominator of $1/p(\alpha)$. This is because α is the root of a minimal degree polynomial $f \in k[X]$. Because $p(\alpha) \neq 0$, f and p are have 1 as their greatest common divisor (because f is irreducible if d divides f then either $d \in k^*$ or $d = f$). So we have $1 = \lambda f + \mu p$ and so $\mu(\alpha) = 1/p(\alpha)$.

The basic object of study is in this course is an algebraic field extension K/k.
Such extensions are defined by polynomial equations: i.e.

Definition 1. *Given K/k, we say that $\alpha \in K$ is algebraic* over *k if it is the solution of an equation of the form $f(\alpha) = 0$ where $f \in k[X]$. We say that K/k is algebraic if each element of K is algebraic over k.*

So for example, $\mathbf{Q}(\pi)/\mathbf{Q}$ is not algebraic and nor is $\mathbf{Q}(e)/\mathbf{Q}$. Likewise for any field k, the function field $k(t)/k$ in one indeterminate t is not algebraic.

We focus on finite extensions: i.e. where $[K : k]$ is finite.
You are presumed to have seen the

Proposition 2. *If K/k is finite, then K/k is algebraic.*

Proof. Sketch: let n be the degree of K/k and let $\alpha \in K$. The elements $\alpha^n, \cdots, 1 \in$ K must satisfy a linear relation over k, $a_n\alpha^n + \cdots + a_1\alpha^1 + a_0$ with $a_i \in k$. Therefore α is a root of the polynomial $f(X) = a_nX^n + \cdots + a_1X + a_0 \in k[X]$. □

Here is an important corollary:

Proposition 3. *1. Let K/L and L/k be algebraic field extensions. Then K/k is an algebraic field extension.*
2. Let K/L and L/k be finite field extensions. Then K/k is a finite field extension.

Proof. We first prove Part 2: this is a consequence of the formula $[K : L][L : k] = [K : k]$. Part 1 follows from Part 2:
If $\alpha \in K$ then there is a monic polynomial $f(X) \in L[X]$ such that $f(\alpha) = 0$. Suppose $f(X) = \sum_i a_i X^i$. For each i we have $g_i \in k[X]$ such that $g_i(a_i) = 0$. Now the field extensions $k(a_1)/k$, $k(a_1, a_2)/k(a_1), \cdots k(a_1, \cdots, a_n)/k(a_1, \cdots, a_{n-1})$ are all finite. Hence $k(a_1, \cdots, a_n)/k$ is finite. Moreover $k(a_1, \cdots, a_n, \alpha)/k(a_1, \cdots, a_n)$ is finite. Therefore $k(a_1, \cdots, a_n, \alpha)/k$ is finite, and so algebraic over k. □

Here is a simple but startling consequence of the previous proposition:
Assume given that π is not algebraic over $\mathbf{Q}$, i.e. there is no non-zero polynomial equation $f \in \mathbf{Q}[X]$ such that $f(\pi) = 0$. (This is the theorem of Lindemann).
Then π is not algebraic over any algebraic extension $K/\mathbf{Q}$. For if it were then it would be algebraic over $\mathbf{Q}$.

We now review some of the basics regarding field extensions and how they are built up using the machinery of algebra. This will be useful for gaining some feeling for splitting fields and their construction.

So far the examples of algebraic extensions we have given have all been finite. It is an important fact that not all algebraic extensions are finite: e.g.

$$K = \mathbf{Q}(\sqrt{p} \mid p \in \mathbf{N} \text{ is prime }).$$

This is a result of the following

Proposition 4. *Let k be a field not of characteristic 2, and let $S = \{a_1, \cdots, a_n\} \subset k^*$ be such that for any subset $T \subset S$*

$$\prod_{i \in T} a_i \notin k^{*2}.$$

Then the field $k(\sqrt{a_1}, \cdots, \sqrt{a_n})$ has degree 2^n over k.

Proof. Proceed by induction on $n = |S|$. If $n = 1$ the theorem is true. Assume, by induction, it is true for $n - 1$, i.e. if $S' \subset k^*$ satisfies the conditions of the theorem and $|S'| = n - 1$, then $k(\sqrt{S'})/k$ has degree 2^{n-1}. By the inductive hypothesis, the theorem is true for the following subsets of k^* which all have cardinality $n - 1$:

$$\begin{aligned} S_1 &= \{a_1, \cdots, a_{n-2}, a_{n-1}\} \\ S_2 &= \{a_1, \cdots, a_{n-2}, a_n\} \\ S_3 &= \{a_1, \cdots, a_{n-2}, a_{n-1}a_n.\} \end{aligned}$$

For convenience write $K = k(\sqrt{a_1}, \cdots, \sqrt{a_{n-2}})$. Therefore if $\sqrt{a_n} \in K(\sqrt{a_{n-1}})$ we have for some $\lambda_1, \lambda_2 \in K$ a relation

$$\sqrt{a_n} = \lambda_0 + \lambda_1 \sqrt{a_{n-1}}$$

which implies that

$$a_n = (\lambda_0^2 + a_{n-1}\lambda_1^2) + 2\lambda_0\lambda_1\sqrt{a_{n-1}}.$$

This means that $\lambda_0\lambda_1 = 0$, by inductive hypothesis as applied to S_1. If $\lambda_0 = 0$ then $\sqrt{a_{n-1}a_n} \in K$, which contradicts the inductive hypothesis as applied to S_3. Therefore $\lambda_1 = 0$, in which case $\sqrt{a_n} \in K$ which contradicts the inductive hypothesis as applied to S_2. □

You are presumed to already have seen the

Definition 5. *Let $f \in k[X]$; a field extension K/k is said to split f if f is a product of linear factors in $K[X]$; such K/k is called a splitting field if is generated by the roots of f, i.e. $K = k(\alpha_1, \cdots, \alpha_n)$ where $f(\alpha_i) = 0$ for each i.*

Example[1]
The field $\mathbf{Q}(i)$ is a splitting field for $X^2+1 \in \mathbf{Q}[X]$. The field $\mathbf{Q}(i, \sqrt{2})$ splits $X^2+1 \in \mathbf{Q}[X]$ but is not a splitting field as $\sqrt{2}$ is not an element of $\mathbf{Q}(i)$.

[1]This was not given in the lecture, but I'll repeat it at the beginning of the next lecture.

Example: the field $\mathbf{Q}(\sqrt{5}, \zeta_5)$

I want to consider the field $K = \mathbf{Q}(\sqrt{5}, \zeta_5)$ where ζ_5 is a primitive 5th root of unity. That is $\zeta_5^5 = 1$ and $\zeta_5^n = 1$ implies that $5 \mid n$.

Then we will show that K is a splitting field for $X^4+X^3+X^2+X+1 = \Phi_5(X)$ considered as a polynomial over $\mathbf{Q}(\sqrt{5})$.

Step 1 is to construct a field isomorphic to $\mathbf{Q}(\sqrt{5})$. We do this as follows:

$$k_1 = \mathbf{Q}[X_1]/(X_1^2 - 5).$$

Now the irreducible polynomial for ζ_5 over $\mathbf{Q}$ is

$$f(X_2) = X_2^4 + X_2^3 + X_2^2 + X_2 + 1$$

because

$$X_2^5 - 1 = (X_2 - 1)f(X_2).$$

(How do we know $f(X_2)$ is irreducible? See this week's exercises to show it is irreducible over $\mathbf{Q}$).

Note, however that the Golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$ and its conjugate satisfy the polynomial equation

$$X_2^2 - X_2 - 1 = 0$$

and so, inspection reveals, we have the factorisation of $f(X)$ over $\mathbf{Q}(\sqrt{5})$:

$$f(X_2) = (X_2^2 + \frac{(1-\sqrt{5})}{2}X_2 + 1)(X_2^2 + \frac{(1+\sqrt{5})}{2}X_2 + 1).$$

The polynomial

$$g(X_2) = X_2^2 + \varphi X_2 + 1$$

has discriminant

$$D(\varphi) = \varphi^2 - 4 = -1 + \sqrt{5}$$

which is not a square in $\mathbf{Q}(\sqrt{5})$, for the squares have the form

$$(a + b\sqrt{5})^2 = (a^2 + b^2 5) + 2ab\sqrt{5}$$

and so the rational part of a square must be positive, but -1 is negative.

We can lift $g(X_2) \in k_1[X_2]$ to an element of $\tilde{g}(X_1, X_2)$ of $\mathbf{Q}[X_1, X_2]$ by

$$\tilde{g} = X_2^2 + \frac{(1 + X_1)}{2}X_2 + 1$$

Hence

$$\mathbf{Q}[X_1, X_2]/(X_1^2 - 5, X_2^2 + \frac{(1 + X_1)}{2}X_2 + 1) \to \mathbf{Q}(\sqrt{5}, \zeta_5) : X_1 \mapsto \sqrt{5}, X_2 \mapsto \zeta_5$$

and moreover

$$\varphi = \zeta_5 + \zeta_5^3,$$

or

$$\varphi = \zeta_5 + \zeta_5^2.$$

So ζ_5 generates K and K contains all the roots of Φ_5 over $\mathbf{Q}(\sqrt{5})$, i.e. it is a splitting field for Φ_5.