

• **The Fundamental Theorem of Galois Theory.**

(cf. Garling, Thm. 11.8, page 97).

Further discussion of the statement of the fundamental theorem of Galois theory.

- More about example (2) of Lecture 1:

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}, \omega),$$

where $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3})$ is a primitive cube root of 1.

Fix a bijection between the sets $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ and $\{1, 2, 3\}$, for example

$$\sqrt[3]{2} \mapsto 1, \quad \sqrt[3]{2}\omega \mapsto 2, \quad \sqrt[3]{2}\omega^2 \mapsto 3.$$

Then we can compute precisely the fixed fields of the subgroups H of G : The subgroup A_3 has index 2 in S_3 and its fixed field is $\mathbf{Q}(\omega)$, which has degree 2 over \mathbf{Q} ;

the fixed field of $\langle(23)\rangle$ is $\mathbf{Q}(\sqrt[3]{2})$;

the fixed field of $\langle(13)\rangle$ is $\mathbf{Q}(\sqrt[3]{2}\omega)$;

the fixed field of $\langle(12)\rangle$ is $\mathbf{Q}(\sqrt[3]{2}\omega^2)$;

• **The separability issue.**

A field \mathbf{K} is said to have $\text{char}(\mathbf{K}) = p$ (necessarily a prime number) if

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0.$$

Examples of such fields \mathbf{K} are:

\mathbf{Z}_p , $\mathbf{Z}_p(x) = \left\{ \frac{f}{g} \mid f, g \in \mathbf{Z}_p[x], g \neq 0 \right\}$, $\mathbf{Z}_p[x]/(f)$, with $f \in \mathbf{Z}_p[x]$ irreducible.

Let \mathbf{K} be a field of characteristic p . Then there exist inseparable extensions of $\mathbf{K}(T)$.

Example. Let \mathbf{K} be the field $\mathbf{Z}_p(T)$. Consider the monic polynomial

$$f(x) = x^p - T \in \mathbf{Z}_p(T)[x].$$

- f is irreducible: this follows by Eisenstein criterion with respect to the prime $T \in \mathbf{Z}_p[T]$, and then by Gauss lemma.

- f is not separable: let α be a zero of f , i.e. an element $\alpha = \sqrt[p]{T}$, in some extension \mathbf{L} of \mathbf{K} . But in characteristic p one has $x^p - T = x^p - \alpha^p = (x - \alpha)^p$. In other words, all roots of f in \mathbf{L} are the same.

As a consequence, the field \mathbf{L} is an inseparable extension of \mathbf{K} : it contains the element α , whose minimal polynomial $x^p - T$ is not separable.