Exercise sheet #3

Prof. Peter Bürgisser, Dr. Pierre Lairez, Paul Breiding and Jesko Hüttenhain

May 4, 2016

Exercise 1. Let K be a field, $f \in K[T]$ an irreducible polynomial and L its splitting field. We assume that the Galois group of the field extension $K \subseteq L$ is abelian. Show that any root $\alpha \in L$ of f generates L over K.
Hint: Show that $K \subseteq K(\alpha)$ *is a normal extension.*

Exercise 2. Let $f = X^4 + uX^2 + v$ be an irreducible polynomial over $\mathbb{Q}$.

1. Show that there are two algebraic numbers α and β such that α, $-\alpha$, β and $-\beta$ are all distinct and are the roots of f.

Let $K = \mathbb{Q}(\alpha, \beta)$, let $U = \{\alpha, -\alpha, \beta, -\beta\}$ and let S be the permutation group of U. Let τ be the transposition $(-\beta, \beta)$ and let ρ be the 4-cycle $(\alpha, \beta, -\alpha, -\beta)$.
Let $D = \left\{\mathrm{id}, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\right\}$ be the subgroup of S generated by τ and ρ. (If the elements of U are distributed on the vertices of a square, then the elements of D can be seen as symmetries and rotations, see Figure 1.)

2. Show that $\mathrm{Gal}(K/\mathbb{Q})$ identifies to a subgroup of D.
3. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is either D, or $\langle\rho\rangle = \left\{1, \rho, \rho^2, \rho^3\right\}$ or $\langle\rho^2, \rho\tau\rangle = \left\{1, \rho^2, \rho\tau, \rho^3\tau\right\}$.
4. Show that $\mathrm{Gal}(K/\mathbb{Q}) = \langle\rho^2, \rho\tau\rangle$ if and only if v is a square in $\mathbb{Q}$.
   Hint: First check that $v = \alpha^2\beta^2$.
5. Show that $\mathrm{Gal}(K/\mathbb{Q}) = \langle\rho\rangle$ if and only if $\frac{u^2}{v} - 4$ is square in $\mathbb{Q}$.
   Hint: First show that $\frac{u^2}{v} - 4 = \left(\frac{\alpha}{\beta} - \frac{\beta}{\alpha}\right)^2$.
6. Describe the subfields of K.
   Hint: First check that the classification of the subgroups of D given in Figure 2 is correct. Then, prove and use repeatedly the following claim: if $B \trianglelefteq A \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$ *and if* $\{\sigma \in B \mid \sigma(t) = t\} = A$ *for some* $t \in K^B$*, then* $K^B = K^A(t)$.
   Check your results by looking at Figure 3.

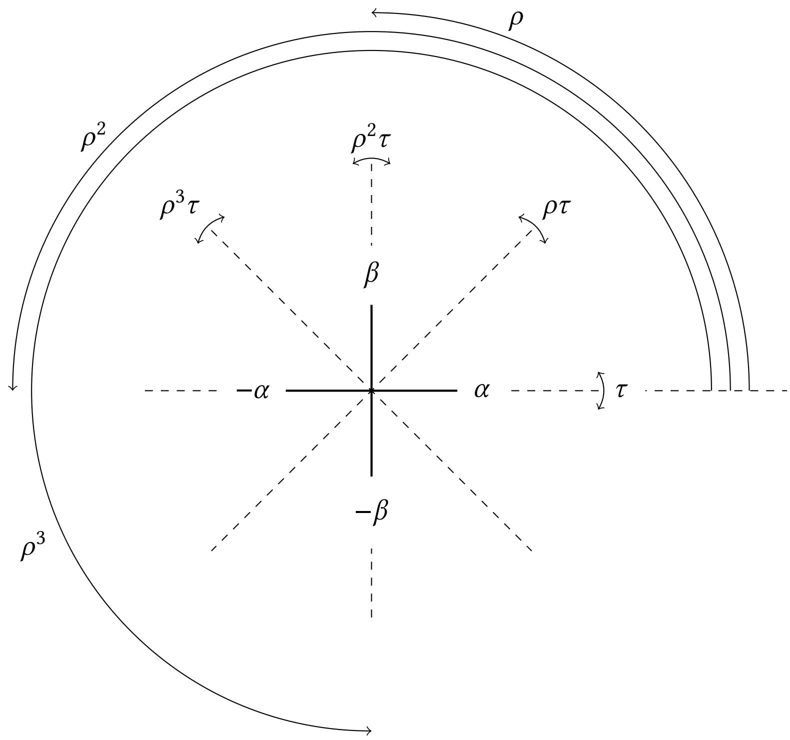

Figure 1: Possible elements of the Galois group of K over $\mathbb{Q}$.

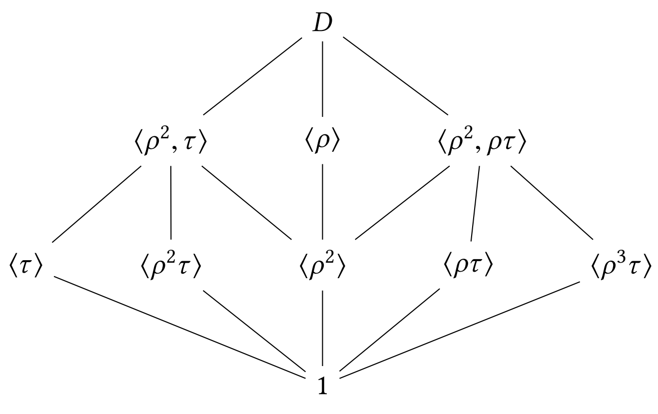

Figure 2: Subgroups of D.

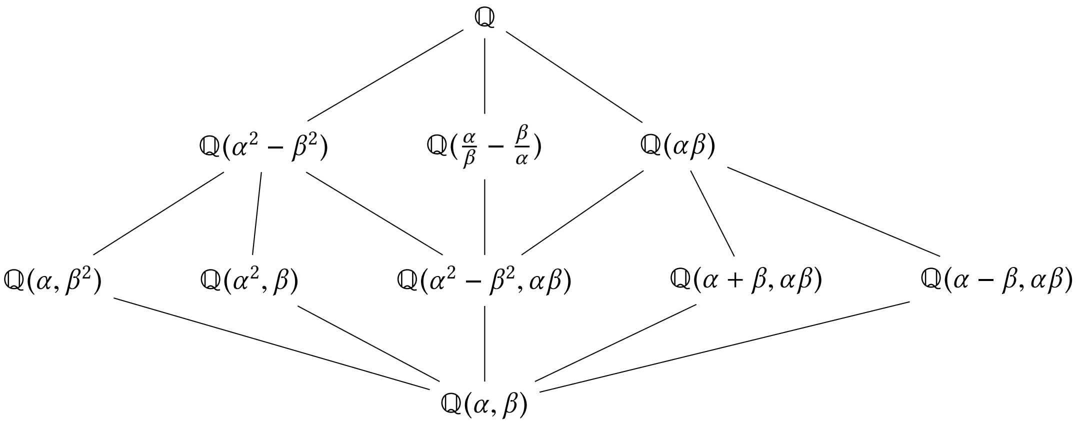

Figure 3: Subfields of $\mathbb{Q}(\alpha, \beta)$.