Kummer theory

Describing the abelian extensions of a general field is very hard, involving things like Class Field Theory and the Kronecker-Weber theorem. Understanding the abelian extensions of a field which contains enough n-th roots of unity is much easier. That is the subject of Kummer theory. We first need some warm ups regarding characters of abelian groups.

Problem 1. (1) List all the characters of the following abelian groups: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) Show that, if A is an abelian group with N elements, then A has precisely N characters.

(3) Show that, if A is an abelian group in which every element obeys $a^M = 1$, and χ is a character of A, then every value of χ is an M-th root of unity.

We write $\hat{A}$ for the set of characters of A. Let $N = \#(A) = \#(\hat{A})$.

(4) Show that, for any $a \in A$, we have

$$\sum_{\chi \in \hat{A}} \chi(a) = \begin{cases} N & a = 1 \\ 0 & a \neq 1 \end{cases}.$$

(5) Show that, for any $\chi \in \hat{A}$, we have

$$\sum_{a \in A} \chi(a) = \begin{cases} N & \chi \text{ trivial} \\ 0 & \chi \text{ non-trivial} \end{cases}.$$

Now, let A be an abelian group with N-elements, and where every element obeys $a^M = 1$. Let F be a field where $N \neq 0$ and containing a primitive M-th root of unity. Thus, all the characters of A can be thought of functions $A \to F^{\times}$. Let K/F be a Galois extension with Galois group A. (Recall that this means that K is a splitting field over F and anything in K which is fixed by $\mathrm{Aut}(K/F)$ is in F.)

Problem 2. Let r be any element of K. Define $r_\chi = \sum_{a \in A} \chi(a)^{-1} \chi(r)$.

(1) Show that

$$r = \frac{1}{N} \sum_{\chi \in \hat{A}} r_\chi.$$

(2) Show that, for $\chi \in \hat{A}$ and $a \in A$, we have $a(r_\chi) = \chi(a) r_\chi$.

(3) Show that r_χ^M is in F.

In conclusion, any element of K is the average of N elements which are M-th roots of elements of F. We now put this into practice.

Problem 3. Let $L = \mathbb{C}(r_1, r_2, r_3)$ with the obvious action of S_3. Let K be the subfield of A_3-invariant elements of L and let F be the subfield of S_3-invariant elements of L.

(1) Write r_1 in the form $\frac{1}{3}\left(e + \sqrt[3]{f_1} + \sqrt[3]{f_3}\right)$, for e, f_1 and f_2 in K. It will turn out, by good luck, that e is in F.

(2) Write f_1 and f_2 in the forms $\frac{1}{2}(u \pm \sqrt{v})$ for u and v in F. You have derived the cubic formula!

Problem 4. Consider the following chain of subgroups of S_4:

$$G_3 = \{e\} \ \subset\ G_2 = \{e, (12)(34), (13)(24), (14)(23)\} \ \subset\ G_1 = A_4 \ \subset\ G_0 = S_4.$$

Let $F_3 = \mathbb{C}(r_1, r_2, r_3, r_4)$, with the obvious action of S_4, and let F_j be the subfield fixed by G_j.

(1) Write r_1 as $\frac{1}{4}\left(e + \sqrt{f_1} + \sqrt{f_2} + \sqrt{f_3}\right)$ for e, f_1, f_2 and f_3 in F_2.

(2) Take each element of F_2 from the previous part and write it in the form $\frac{1}{3}\left(g + \sqrt[3]{h_1} + \sqrt[3]{h_2}\right)$ for g, h_1 and h_2 in F_1.

(3) Take each element of F_3 from the previous part and write it as $\frac{1}{2}\left(u \pm \sqrt{v}\right)$ for u and v in F_0. You have derived the quartic formula!

Problem 5. Let A be $\mathbb{Z}_m$, and keep all notation as above. Let ζ_m be a primitive m-th root of unity in $F^\times$, and let χ be the character $\chi(a) = \zeta_m^a$ of A.

(1) Show that there is some element r of K with $r_\chi \neq 0$.

(2) Show that there is some $u \in F$ such that $K = F(u^{1/m})$. This is the result usually called **Kummer's theorem**.