## GALOIS THEORY 2015/2016 EXERCISE SHEET 6

Questions marked with a star are optional.

(1) (a) Show that for any field $K$, and any positive integer $n$, the number of $n$th roots of unity in $K$, i.e. the number of $x$ in $K$ such that $x^n = 1$, is a divisor of $n$.
(b) Using the classification of finite abelian groups, deduce that for any field $F$, any finite subgroup of $F^\times$ is cyclic.

(2) Recall that we saw in lectures that the cyclotomic polynomial $\Phi_n(X)$ is irreducible, and deduced that $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ is Galois of degree $\varphi(n)$, with Galois group

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod (\mathbb{Z}/p_i^{n_i})^\times,$$

where $n = \prod p_i^{n_i}$ is the decomposition of $n$ into its prime factors.
(a) Show that for any finite abelian group $G$, there exists a set of primes $p_1, \ldots, p_m$, and a surjective group homomorphism

$$\prod_{i=1}^{m} \mathbb{Z}/(p_i - 1)\mathbb{Z} \to G.$$

(You may use Dirichlet's Theorem on primes in arithmetic progressions without proving it!)
(b) Deduce that for any finite abelian group $G$, there exists a Galois extension $L|\mathbb{Q}$ such that

$$\mathrm{Gal}(L|\mathbb{Q}) \simeq G.$$

(3) Let $m$ be an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $k$ denote the order of $m$ in the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $H$ denote the subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ generated by the automorphism

$$\zeta \mapsto \zeta^m$$

Let $L = \mathbb{Q}(\zeta_n)^H$.
(a) For every $n$th root of unity $\zeta$, define

$$\alpha(\zeta) := \sum_{i=0}^{k-1} \zeta^{m^i}.$$

Show that for every such $\zeta$, $\alpha(\zeta)$ is an element of $\mathbb{Q}(\zeta_n)$, and that $L$ is generated by the set $\{\alpha(\zeta):\zeta \text{ a primitive } n\text{th root of unity }\}$.
(b) Using part (a), find an extension of $\mathbb{Q}$ which is Galois with Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (here 'find' can be taken to mean: write down elements $\alpha_1, \ldots \alpha_n$ in $\mathbb{C}$ such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.)
(c) *Show that $L = \mathbb{Q}(\alpha(\zeta))$ for any primitive $n$th root of unity $\zeta$.

Comments, corrections, questions etc to netandogra@gmail.com.