HOMEWORK 9

DUE 14 MARCH 2014

1. Let K be the splitting field of $f(x) = x^6 + 2$ over $\mathbb{Q}$. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ whose matrices have the form $\begin{pmatrix} \pm 1 & * \\ 0 & 1 \end{pmatrix}$. Under this isomorphism, which matrix corresponds to complex conjugation? What is the fixed field of complex conjugation? In what way does the problem (and its solution) change if you consider the splitting field of $g(x) = x^6 + 3$ instead?

2. Let $K = \mathbb{Q}(\zeta_{16})$ be the field of 16-th roots of unity.

(a) Which of the fields $\mathbb{Q}(\sqrt{2}\,)$, $\mathbb{Q}(\sqrt[4]{2}\,)$, $\mathbb{Q}(\sqrt{2+\sqrt{2}}\,)$, and $\mathbb{Q}(\sqrt{2+\sqrt{-2}}\,)$ are contained in K?

(b) Find all the subfields of K, and identify each of them as the fixed field of a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.

3. Suppose $K/\mathbb{Q}$ is a finite Galois extension with Galois group G. Let $\alpha \in K$.

(a) The *norm* of α is defined to be $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Show that $N(\alpha) \in \mathbb{Q}$.

(b) We call $\beta \in K$ an *algebraic integer* if its monic irreducible polynomial $\mathrm{Irr}(\beta, \mathbb{Q}, x) \in \mathbb{Q}[x]$ has coefficients in $\mathbb{Z}$. For any algebraic integer β, show that $|N(\beta)| \geq 1$.

(c) A positive integer d is called a *denominator* for α if $d\alpha$ is an algebraic integer. Show that α has a denominator.

(d) Let d be the smallest denominator for α and define

$$s(\alpha) = \max\left\{\log d, \log|\sigma\alpha|; \sigma \in G\right\}.$$

Show that $s(\alpha) \geq 0$ and that $s(\alpha_1\alpha 2) \leq s(\alpha_1) + s(\alpha_2)$.

(e) For any $\sigma \in G$ and $\alpha \in K$, show that $-2[K : \mathbb{Q}]s(\alpha) \leq \log|\sigma\alpha|$. What do you think this means?

4. Let L/K be a finite Galois extension. Let $w_1, \ldots, w_d \in L$ be a basis for L as a K-vector space. Let $\sigma_1, \ldots, \sigma_d$ be the elements of the Galois group of L/K. Let

$$M = \begin{pmatrix} \sigma_1(w_1) & \ldots & \sigma_1(w_d) \\ \vdots & & \vdots \\ \sigma_d(w_1) & \ldots & \sigma_d(w_d) \end{pmatrix}.$$

Show that $\det(M)^2 \in K^\times$.

Inverse limits

From Dummit and Foote: section **7.6** problems 10, 11. For 11, show that the maps defined at the beginning of 11 form an inverse system and therefore you can take the inverse limit to define $\mathbb{Z}_p$. Also note that they define the inverse limits for groups, and therefore their inverse limit is a priori only a group. So you will have to show that $\mathbb{Z}_p$ is a ring, and in particular multiplication is well defined. The ring $\mathbb{Z}_p$ called the ring of p-adic integers.

5. Let $\mathbb{N}$ be the set of positive integers ordered by divisibility. Observe that

$$\{\mathbb{Z}/n\mathbb{Z}\}_{n\in\mathbb{N}}$$

forms an inverse system of commutative rings with the canonical homomorphisms

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \text{ for } m \mid n.$$

Let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. Again, this is a priori only a group. (In fact, inverse and direct limits can be defined more generally in a category, and in particular in the category of rings.) Show that $\hat{\mathbb{Z}}$ is a ring with the natural multiplication and that

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

6. Let p be a prime and let $\mathbb{F}_p$ be a field with p elements.

(a) Show that $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. (Use the shortest proof possible...)

(b) Let $K/\mathbb{F}_p$ be a finite extension. Then K is a finite dimensional vector space over $\mathbb{F}_p$ and hence has $q = p^n$ elements for some n. Show that $K/\mathbb{F}_p$ is Galois with cyclic Galois group generated by

$$\phi : K \longrightarrow K, x \mapsto x^p.$$

As you probably already know, ϕ is called the p-th power Frobenius.

(c) Show that for each $n \geq 1$, there is exactly one field K, with $\mathbb{F}_p \subseteq K \subseteq \bar{\mathbb{F}}_p$ of degree n over $\mathbb{F}_p$.

(d) Show that $\mathrm{Gal}\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right) \cong \hat{\mathbb{Z}}$. (It is also true that $\mathrm{Gal}\left(\bar{\mathbb{F}}_q/\mathbb{F}_q\right) \cong \hat{\mathbb{Z}}$ with the same proof.)