Student seminar exercise sheet Week 12

1. In this exercise you finish the proof of Proposition 5.7, from Nancy Childress's book.
   Let K/F be a Galois extenion of number fields, with cyclic Galois group $G = \langle \sigma \rangle$. Let v be a place of F and w be a place of K above v. We define $\mathcal{S} := \{v \in V_F : v \text{ is infinite, or } v \text{ramifies in } K/F\}$. We want to show that

   $$\mathcal{Q}_G \left(\prod_{v \notin \mathcal{S}} \prod_{w|v} \mathcal{U}_w \right) = 1$$

   .

   (a) Define $A = \prod_{v \notin \mathcal{S}} A_v$, where $A_v = \prod_{w|v} \mathcal{U}_w$, and notice that $\mathcal{S}$ is a finite set. Show that $A_v^G \cong \mathcal{U}_v$ and $s(G)A_v \cong \mathcal{U}_v$.

   (b) Show that $[\ker_{A_v} s(G) : (\sigma - 1)A_v] = 1$.

   (c) Show that $A^G = s(G)A$ and $\ker_A s(G) = (\sigma - 1)A$, and conclude.

2. This exercise will prove lemma 5.9 of Nancy Childress's book.
   Let G be a finite group acting on a finite set $\mathcal{S}$. Let

   $$V = \bigoplus_{w \in \mathcal{S}} \mathbb{R} X_w$$

   be a vector space. Then G acts on V via

   $$\sigma \left(\sum_{w \in \mathcal{S}} a_w X_w \right) = \sum_{w \in \mathcal{S}} a_w X_{\sigma w}.$$

   Let $\mathcal{L} \subseteq V$ be a lattice preserved by G. You will show in this exercise that there exists a basis $\{Y_w\}_{w \in \mathcal{S}}$ of V contained in $\mathcal{L}$ such that $\sigma(Y_w) = Y_{\sigma w}$, for all $\sigma \in G$, $w \in \mathcal{S}$.

   For any $\sum_{w \in \mathcal{S}} a_w X_w \in V$, define the following norm on V :

   $$|| \sum_{w \in \mathcal{S}} a_w X_w ||_0 = \max_w \{|a_w| : w \in \mathcal{S}\}.$$

   To prove this exercise use lemma 5.8 from the book, which states that if we have a set $\{X'_w\}_{w \in \mathcal{S}}$ such that for every $w \in \mathcal{S}$ $||X'_w - X_w||_0 < \frac{1}{\dim_{\mathbb{R}} V}$, then $\{X'_w\}_{w \in \mathcal{S}}$ is also a basis for V.

(a) Let $\{w_1, ..., w_r\}$ to be a complete set of representatives for the orbits of the action of G on $\mathcal{S}$. Show that for $i \in \{1, \dots, r\}$ we can choose elements $X'_{w_i} \in \mathbb{Q}\mathcal{L}$ such that

$$||X'_{w_i} - X_{w_i}||_0 < \frac{1}{\dim_{\mathbb{R}} V}$$

.

(b) Define for all $i \in \{1, \dots, r\}$

$$X''_{w_i} = \frac{1}{|G_{w_i}|} \sum_{\sigma \in G_{w_i}} \sigma(X'_{w_i}),$$

where $G_{w_i} := \{\sigma \in G | \sigma(w_i) = w_i\}$, and show that $||X''_{w_i} - X_{w_i}||_0 < \frac{1}{\dim_{\mathbb{R}} V}$.

(c) Show that defining X''_w to be $\sigma(X''_{w_i})$ whenever $\sigma w_i = w$ is a definition that makes sense. In particular a similar definition would not have made sense on the X'_{w_i}'s.

(d) Show that $\{X''_w\}_{w \in \mathcal{S}}$ is a basis of V contained in $\mathbb{Q}\mathcal{L}$ and that we can transform it into a basis contained in $\mathcal{L}$.

(e) Call the basis found in the previous point $\{Y_w\}_{w \in \mathcal{S}}$, and show that $\sigma(Y_w) = Y_{\sigma w}$, for any $\sigma \in G$, $w \in \mathcal{S}$. This will conclude the proof of the lemma.

3. Let K/F be an abelian extension of number fields, and let $\mathfrak{f} = \mathfrak{f}(K/F)$.

(a) Show: if $\mathfrak{m}$ is an ideal of $\mathcal{O}_F$ such that $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$, then $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$.

(b) Prove or disprove and salvage: If $\mathcal{E}^+_{F,\mathfrak{m}} \subseteq F^\times N_{K/F} J_K$, then

$$\mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F}(\mathfrak{m}) \;=\; \mathcal{P}^+_{F,\mathfrak{f}} \mathcal{N}_{K/F}(\mathfrak{f}) \cap \mathcal{I}_F(\mathfrak{m}).$$

(c) Suppose $\mathcal{I}_F(\mathfrak{m}) \subseteq \mathcal{I}_F(\mathfrak{f})$. Show that there is a natural embedding

$$\mathcal{I}_F(\mathfrak{m})/\mathcal{P}^+_{F,\mathfrak{m}} N_{K/F}(\mathfrak{m}) \;\hookrightarrow\; \mathcal{I}_F(\mathfrak{f})/\mathcal{P}^+_{F,\mathfrak{f}} N_{K/F}(\mathfrak{f})$$

induced by inclusion.

(d) Under what circumstances is the embedding of part (c) an isomorphism?

4. Let $K = \mathbb{Q}(\sqrt{5}, i)$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where σ is complex conjugation, while τ fixes i and sends $\sqrt{5} \mapsto -\sqrt{5}$. Suppose $p\mathbb{Z}$ is an unramified prime in $K/\mathbb{Q}$.

(a) Compute

$$\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right),$$

i.e., give congruence conditions on p that determine whether the Artin symbol is 1, σ, τ, or $\sigma\tau$. (Hint: If you can find some cyclotomic field that contains K, then Example 1 of Chapter 1 may be useful.)

(b) Give necessary and sufficient conditions (in terms of congruence) on $p\mathbb{Z}$ to split completely in $K/\mathbb{Q}$. Compare your answer with (a) and Theorem 1.18:

Theorem 0.1. *Let $K \subseteq \mathbb{Q}(\zeta_m)$, then identify $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and let $H < (\mathbb{Z}/m\mathbb{Z})^\times$ be the subgroup corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$. The primes $p \nmid m$ that split completely in $K/\mathbb{Q}$ are precisely the unramified primes with trivial Artin automorphism.*

(c) Suppose $p\mathbb{Z}$ is inert in $\mathbb{Q}(i)/\mathbb{Q}$. What can you say about

$$\left(\frac{p\mathbb{Z}[i]}{K/\mathbb{Q}(i)}\right)?$$

(d) Suppose $p\mathbb{Z}$ splits in $\mathbb{Q}(i)/\mathbb{Q}$, say $p\mathbb{Z}[i] = \mathfrak{p}\mathfrak{p}'$. What can you say about

$$\left(\frac{p}{K/\mathbb{Q}(i)}\right)?$$