GALOIS COHOMOLOGY
EXERCISES 12

Let k be a field.

Exercise 1. Let $n \geq 1$ be an integer, and $\omega \in k$ a root of unity of order n. Let $a, b \in k^\times$. Consider the Galois $\mathbb{Z}/n$-algebra $R_a = k[X]/(X^n - a)$, where $i \in \mathbb{Z}/n$ acts by $X \mapsto \omega^i X$. Up to isomorphism R_a depends only on the class of a in $k^\times / k^{\times n}$ (and on n and the choice of ω). Let us denote the cyclic algebra (R_a, b) by $(a, b)_\omega$.

(i) Show that $(a,b)_\omega \simeq ((b,a)_\omega)^{\mathrm{op}}$.
(ii) If $a \neq 1$, show that $(1-a, a)_\omega \simeq M_n(k)$.

We define the extension $K = k(\sqrt[n]{a})$ as the splitting field of the polynomial $X^n - a \in k[X]$.

(iii) Show that $R_a \simeq K \times \cdots \times K$ as k-algebras.
(iv) Show that $N_{R_a/k}(R_a^\times) = N_{K/k}(K^\times)$ in $k^\times$.
(v) Prove the "reciprocity law":

$$a \in \mathrm{N}_{k(\sqrt[n]{b})/k}(k(\sqrt[n]{b})) \Longleftrightarrow b \in \mathrm{N}_{k(\sqrt[n]{a})/k}(k(\sqrt[n]{a})).$$

Exercise 2. Let $\overline{k}$ be an algebraic closure of k. We first assume that $\overline{k}/k$ is finite of prime order p, where p is unequal to the characteristic of k.

(i) Show that $\overline{k}$ is generated by an element α such that $a = \alpha^p \in k$.
(ii) Show that $\mathrm{Br}(\overline{k}/k) \simeq H^2(k, \mathbb{Z}/p)$ and $k^\times/k^{\times p} \simeq H^1(k, \mathbb{Z}/p)$, and that each of these groups is isomorphic to $\mathbb{Z}/p$. (Hint: Use the computation of the cohomology of finite cyclic groups.)
(iii) Deduce that $N_{\overline{k}/k}(\overline{k}^\times) = k^{\times p}$.
(iv) Show that $\mathrm{N}_{\overline{k}/k}(\alpha) = (-1)^{p-1} a$.
(v) Deduce that $p = 2$, that -1 is not a square in k, and that $\overline{k} \simeq k[X]/(X^2+1)$.

We now assume that $\overline{k}/k$ is finite (of possibly nonprime order) and that k has characteristic zero.

(vi) Assume that -1 is a square in k. Show that $k = \overline{k}$.
(vii) Assume that -1 is not a square in k. Show that $\overline{k} \simeq k[X]/(X^2+1)$.