GALOIS COHOMOLOGY
EXERCISES 1 (TENSOR PRODUCT)

Let k be a field and U, V be k-vector spaces. Let us denote by F the k-vector space having as basis the set $U \times V$; it consists of k-linear combinations of elements of type (u, v) with $u \in U$ and $v \in V$. Consider the subspace R of F generated by the following elements

$$(u + \lambda u', v + \mu v') - (u, v) - \lambda(u', v) - \mu(u, v') - \lambda\mu(u', v'),$$

where $u, u' \in U$ and $v, v' \in V$ and $\lambda, \mu \in k$. The quotient k-vector space F/R will be denoted by $U \otimes_k V$, and the image of (u, v) by $u \otimes v \in U \otimes_k V$.

Exercise 1. Let W be another k-vector space and $\varphi \colon U \times V \to W$ a map. Assume that φ is k-bilinear, i.e. that for all $u \in U$ the map $V \to W$ given by $v \mapsto \varphi(u, v)$ is k-linear and for all $v \in V$ the map $U \to W$ given by $u \mapsto \varphi(u, v)$ is k-linear. Show that there is a unique k-linear map $U \otimes_k V \to W$ sending $u \otimes v$ to $\varphi(u, v)$ for all $u \in U$ and $v \in V$.

Exercise 2.
- (i) Assume that the elements e_α for $\alpha \in A$ form a basis of U, and that f_β for $\beta \in B$ form a basis of V. Show that the elements $e_\alpha \otimes f_\beta$ for $(\alpha, \beta) \in A \times B$ form a basis of $U \otimes_k V$. (Hint: for linear independence, use the dual basis to (e_α) and (f_β) to define linear forms $U \otimes_k V \to k$.)
- (ii) If $U \neq 0$ and $V \neq 0$, show that $U \otimes_k V \neq 0$.
- (iii) Assume that $\dim_k U = m < \infty$ and that $\dim_k V = n < \infty$. What is the dimension of $U \otimes_k V$?

Exercise 3. Let $f \colon U \to U'$ and $g \colon V \to V'$ be k-linear maps.
- (i) Show that there is a unique k-linear map

$$f \otimes g \colon U \otimes_k V \to U' \otimes_k V'$$

  such that

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v) \quad \text{for all } u \in U \text{ and } v \in V.$$

- (ii) Assume that f and g are surjective. Show that $f \otimes g$ is surjective.
- (iii) Assume f and g are injective. Show that $f \otimes g$ is injective.

Exercise 4. Assume that A, B are k-algebras. Show that $A \otimes_k B$ is naturally a k-algebra.

Exercise 5. When $f\colon U \to V$ and $g\colon V \to W$ are k-linear maps, we say that the sequence

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

is exact if f is injective, g is surjective, and $\ker g = \operatorname{im} f$. If F is a k-vector space, show that the induced sequence

$$0 \to U \otimes_k F \xrightarrow{f \otimes \mathrm{id}} V \otimes_k F \xrightarrow{g \otimes \mathrm{id}} W \otimes F \to 0$$

is exact.

Exercise 6. If $U' \subset U', V' \subset V$ are subspaces, by Exercise 3 (iii) we may view $U' \otimes_k V'$ as a subspace of $U \otimes_k V$.

(i) Assume that U_α for $\alpha \in A$ are subspaces of U such that $U = \bigoplus_{\alpha \in A} U_\alpha$. Show that

$$U \otimes_k V = \bigoplus_{\alpha \in A} (U_\alpha \otimes V).$$

(ii) Let U', U'' be subspaces of U. Show that, in $U \otimes_k V$,

$$(U' \otimes_k V) \cap (U'' \otimes_k V) = (U' \cap U'') \otimes_k V.$$

(iii) If $U' \subset U$ and $V' \subset V$ are subspaces, show that, in $U \otimes_k V$,

$$(U' \otimes_k V) \cap (U \otimes_k V') = U' \otimes_k V'.$$

GALOIS COHOMOLOGY
EXERCISES 2 (QUATERNIONS)

Let k be a field of characteristic $\neq 2$.

Exercise 1. Let $a \in k^\times$. Show that:

(i) $(a, -a)$ splits.
(ii) If $a \neq 1$, then $(a, 1-a)$ splits.
(iii) $(a, a) \simeq (a, -1)$.
(iv) $(a, -1)$ splits if and only if a is a sum of two squares in k.

Exercise 2. (Chain Lemma.) Let $a, b, c, d \in k^\times$ be such that $(a, b) \simeq (c, d)$. We are going to prove that there is $e \in k^\times$ such that

$$(a, b) \simeq (e, b) \simeq (e, d) \simeq (c, d).$$

So we let Q be such that $(a, b) \simeq Q \simeq (c, d)$.

(i) Let i, j, resp. i', j', be the images in Q of the standard generators of (a, b), resp. (c, d). Show that $i, j, i', j' \in Q_0$.
(ii) Let V be the k-subspace of Q_0 generated by j, j'. Show that the morphism $\varphi\colon Q_0 \to \mathrm{Hom}_k(V, k)$ sending $q \in Q_0$ to the map $v \mapsto qv + vq$ is not injective.
(iii) Deduce that there is a nonzero $\varepsilon \in Q_0$ such that $\varepsilon j = -j\varepsilon$ and $\varepsilon j' = -j'\varepsilon$.
(iv) Show that $e = \varepsilon^2 \in k$, and conclude.

Exercise 3. Let L/k be a field extension of odd degree and Q a quaternion k-algebra. Show that Q splits if and only if $Q \otimes_k L$ splits over L. (Hint : use the splitting criterion involving the norm of quadratic field extensions, and the properties of field norms.)

GALOIS COHOMOLOGY
EXERCISES 3 (QUATERNIONS)

Let k be a field of characteristic $\neq 2$.

Exercise 1. Show that every quaternion algebra can be realised as a subalgebra of $M_4(k)$.

Exercise 2. Let $k = \mathbb{Q}$, and consider that quaternion algebra $Q = (-1, -1)$ over k. Let $K = k(\xi)$ where $\xi \in \mathbb{C}$ is a primitive 5-th root of 1.

(i) Show that Q_K splits. (Hint : compute $-(\xi^3 + \xi^2)^2 - (\xi - \xi^4)^2$.)
(ii) Determine the subfields of K.
(iii) Deduce that K contains no quadratic extension splitting Q.

Exercise 3. Show that every element of a quaternion k-algebra satisfies a quadratic equation over k.

Exercise 4. Let D be a division k-algebra. We assume that for every $d \in D$, there is a nonzero polynomial $P \in k[X]$ of degree ≤ 2 such that $P(d) = 0$. We are going to prove that one of the following must happen:

— $D = k$,
— D is a quadratic field extension of k,
— D is a quaternion k-algebra.

Let us assume that $D \neq k$.

(i) Show that there is $i \in D - k$ and $a \in k$ such that $i^2 = a$.
(ii) Let K be the k-subalgebra of D generated by i. Show that K is a field and that $[K : k] = 2$.
(iii) Let $\varphi\colon D \to D$ be the map $d \mapsto i^{-1}di$. Show that $\varphi^2 = \mathrm{id}$, and that $D = D_+ \oplus D_-$ as K-vector spaces, where $D_+ = \ker(\varphi - \mathrm{id})$, $D_- = \ker(\varphi + \mathrm{id})$.
(iv) Show that D_+ is a K-subalgebra of D.
(v) Let $\alpha \in D_+$ and F the K-subalgebra of D_+ generated by α. Show that F is a field.
(vi) Show that $\alpha \in K$. (Hint: use the minimal polynomials of α and $\alpha + i$ to construct a linear equation over K having α as a solution.)
(vii) Deduce that $D_+ = K$.
(viii) Let now $\beta, \beta' \in D_-$. Show that $\beta\beta' \in D_+$, and deduce that $\dim_K D_- \in \{0, 1\}$.
(ix) Assume that $\dim_K D_- = 1$, and let j be a nonzero element of D_-. Let $A \in k[X]$ be a nonzero polynomial of degree ≤ 2 such that $A(j) = 0$. Show that $A(-j) = 0$, and deduce that $j^2 \in k$.
(x) Conclude.

GALOIS COHOMOLOGY
EXERCISES 4 (SIMPLE RINGS)

Exercise 1. Prove the following converse of Wedderburn's Theorem: If D is a division ring and $n \geq 1$ an integer, then the ring $M_n(D)$ is artinian simple.

Exercise 2. In Proposition 1.3.5, we proved the following statement : if Q, Q' are quaternion algebras over a field k (of characteristic $\neq 2$), then

$$Q \otimes_k Q' \simeq M_4(k) \Longleftrightarrow Q \simeq Q'.$$

The proof of "$\Longleftarrow$" was easy, while the proof of "$\Longrightarrow$" was comparatively difficult (in particular used Albert's Theorem). Give a new (short) proof of "$\Longrightarrow$", using "$\Longleftarrow$" and the results of §2.1 in the lecture notes.

Exercise 3. Let R be a ring and $n \in \mathbb{N} - 0$. Show that R and $M_n(R)$ have the same center.

Exercise 4. (i) Show that every nonzero ring admits a simple module.

(ii) Let R be a ring, and M a nonzero R-module. Show that there is a submodule N of M and a quotient S of N such that S is simple.

Exercise 5. Let D be a division algebra of positive characteristic (i.e. there is a prime number p such that $pD = 0$.) Show that every finite subgroup of $D^\times$ is cyclic. (Hint: you may use the fact that every subgroup of $k^\times$ is cyclic when k is a finite field).

GALOIS COHOMOLOGY
EXERCISES 5 (SEMISIMPLE RINGS)

Exercise 1. Let k be a field. Let D be a finite-dimensional central division k-algebra and L/k a finite field extension such that $\operatorname{ind}(D) = [L : k]$. Show that L is a splitting field for D if and only if L can be embedded in D. (Hint: Look at the proof of Proposition 2.5.2 in the notes.)

Exercise 2. Let R be a ring and M an R-module. We are going to prove that the following conditions are equivalent:

(a) The module M is generated by its simple submodules.
(b) The module M is a direct sum of simple R-modules.
(c) Every submodule of M is a direct summand.

The R-module M will be called *semisimple* if it satisfies the above conditions.

(i) Let $S_i \to M$ for $i \in I$ be a collection of morphisms of R-modules, where each S_i is a simple module. When $K \subset I$, let us write $S_K = \bigoplus_{i \in K} S_i$, and denote by N_K the kernel of $S_K \to M$. Using Zorn's lemma, show that there is a maximal subset $K \subset I$ such that $N_K = 0$.
(ii) In the situation of (i), show that $S_I \to M$ and $S_K \to M$ have the same image.
(iii) Prove that (a) $\Longrightarrow$ (b).
(iv) Prove that (b) $\Longrightarrow$ (c). (Hint: use (i) and (ii) for an appropriate collection of morphisms $S_i \to Q$.)

For the rest of the exercise, we assume that (c) holds, and prove (a). So we let M' be the submodule of M generated by the simple submodules of M, and choose a submodule M'' such that $M' \oplus M'' = M$. We assume that $M'' \neq 0$ and come to a contradiction. By a previous exercise, we know that there are submodules $P \subset N \subset M''$ such that N/P is simple.

(v) Show that N/P is isomorphic to a submodule of N. (Hint: Introduce a submodule Q such that $P \oplus Q = M$.)
(vi) Conclude that (c) $\Longrightarrow$ (a).

Exercise 3. A ring is called *semisimple* if it is semisimple as a module over itself (see the previous exercise). Prove the following assertions:

(i) Every semisimple ring is a finite direct sum of simple modules.
(ii) Every semisimple ring is artinian.
(iii) Every artinian simple ring is semisimple.
(iv) Every semisimple ring is isomorphic to a product $M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where $D_1, \ldots, D_r$ are division algebras and $n_1, \ldots, n_r$ are integers. (Hint: Proceed as in the proof of Wedderburn's Theorem.)
(v) The product of two semisimple rings is semisimple.
(vi) A ring is semisimple if and only if it is a finite product of artinian simple rings.

GALOIS COHOMOLOGY
EXERCISES 6 (SEPARABLE SPLITTING FIELDS)

The letter k denotes a field. The purpose of this exercise sheet it to describe another proof of the fact that every finite-dimensional central division k-algebra contains a maximal subfield which is separable over k. This alternative approach is longer (and for this reason was not included in the notes), but is in a sense much more natural if one is familiar with algebraic geometry. It can also more easily be adapted to prove other statements in the same vein.

The first exercise contains a construction of the discriminant of a polynomial. If you already know about this (or are not interested), you can skip to Exercise 2, which use only the fact stated in (iii) of Exercise 1.

Exercise 1. (i) Let $P = p_n X^n + \cdots + p_0$ and $Q = q_m X^m + \cdots + q_0$ be polynomials in $k[X]$. Construct a matrix $S \in M_{m+n}(k)$ having the following property. If $A = a_{m-1}X^{m-1} + \cdots + a_0$ and $B = b_{n-1}X^{n-1} + \cdots + b_0$ are polynomials in $k[X]$, writing

$$S \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} u_{m+n-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ u_0 \end{pmatrix}$$

we have

$$PA + QB = u_{m+n-1}X^{m+n-1} + \cdots + u_0 \in k[X].$$

(ii) Assume that $p_n \neq 0$ and $q_m \neq 0$. Show that P and Q admit a nontrivial common factor if and only if $\det S = 0$. (The value $\det S$ is called the *resultant* of P and Q.)

(iii) Fix an integer d. Show that there exists a polynomial $\delta \in k[X_0, \dots, X_d]$ such that $\delta(a_0, \dots, a_d) \neq 0$ if and only if the polynomial $a_d X^d + \cdots + a_0$ is separable. (Hint: a polynomial is separable if and only if it is prime to its derivative.)

Exercise 2. Let A be a finite-dimensional k-algebra and $a \in A$. The kernel of the k-algebra morphism $k[X] \to A$ is a principal ideal. Recall that the *minimal polynomial* of a is the unique generator of that ideal having leading coefficient 1.

(i) Let L/k be a field extension. If $P \in k[X]$ is the minimal polynomial of a in the k-algebra A, show that its image $P \in L[X]$ is the minimal polynomial of $a \otimes 1$ in the L-algebra $A \otimes_k L$.

(ii) Let $M \in M_n(k)$ and $\chi \in k[X]$ its characteristic polynomial. Show that if χ is separable, then χ is the minimal polynomial of M.

(iii) Fix an integer n. Show that there exists a polynomial $\pi \in k[X_{i,j}, 1 \leq i, j \leq n]$ having the following property: if M is a matrix in $M_n(k)$ having coefficients $m_{i,j} \in k$ for $1 \leq i, j \leq n$, then $\pi(m_{1,1}, \ldots, m_{n,n}) \neq 0$ if and only if the minimal polynomial of $M \in M_n(k)$ is separable of degree n. (Hint : use (iii) of the previous exercise.)

Let now D be a central division k-algebra of degree n, and F an algebraic closure of k.

(iv) Let $e_1, \ldots, e_{n^2}$ be a k-basis of D. Show that there exists a polynomial $\rho \in F[X_1, \ldots, X_{n^2}]$ having the following property: if $x \in D$ has coefficients $x_1, \ldots, x_{n^2}$ in the basis $e_1, \ldots, e_{n^2}$, then $\rho(x_1, \ldots, x_{n^2}) \neq 0$ if and only if the minimal polynomial of x in the k-algebra D is separable of degree n.

(v) Assume that k is infinite. Let L/k be a field extension and d an integer. Let $P \in L[X_1, \ldots, X_d]$ be a polynomial. Assume that there exist $y_1, \ldots, y_d \in L$ such that $P(y_1, \ldots, y_d) \neq 0$. Show that there exist $x_1, \ldots, x_d \in k$ such that $P(x_1, \ldots, x_d) \neq 0$. (Hint: find $x_1, \ldots, x_m \in k$ by induction on m so that $P(x_1, \ldots, x_m, y_{m+1}, \ldots, y_d) \neq 0$.)

(vi) Conclude that D contains a separable extension of k of degree n. (Hint: observe that the case when k is finite is easy.)

GALOIS COHOMOLOGY
EXERCISES 7 (PROFINITE GROUPS)

Exercise 1. Let us fix a prime number p.

(i) Let G be a profinite group, and $P \subset G$ a pro-p-Sylow subgroup. Show that:
- for every normal open subgroup U of G containing P, the group G/U has finite order prime to p,
- if $H \subset P$ is a closed subgroup of finite index in P, then $[P : H]$ is a power of p.

(ii) Let k be a field. Show that there exists a separable field extension F/k having the following properties:
- every finite subextension L/k of F/k has degree prime to p,
- the degree of every finite separable extension of F is a power of p.

Exercise 2. Recall that a topological space is called *Hausdorff* if any two distinct points are contained in disjoint opens subsets.

(i) Let Γ be a profinite group. We have seen that Γ is compact. Show that Γ is Hausdorff and that every open subset of Γ containing 1 contains an open normal subgroup.

Let now G be a compact and Hausdorff topological group. We assume that every open subset of G containing 1 contains an open normal subgroup. We are going to show that G is profinite. Let $\mathcal{U}$ be the set of open normal subgroups of G, ordered by setting $U \leq V$ when $V \subset U$.

(ii) Show that the groups G/U for $U \in \mathcal{U}$ form an inverse system, that the group $H = \varprojlim G/U$ is profinite and that the natural morphism $f: G \to H$ is continuous.

(iii) Show that f is injective.

(iv) Show that the image of f is dense (i.e. meets every nonempty open subset of H).

(v) Conclude that $f: G \to H$ is a homeomorphism.

Exercise 3. A topological space all of whose connected subsets are singletons is called *totally disconnected*. We are going to prove that a topological space is profinite if and only it is compact, Hausdorff, and totally disconnected.

(i) Show that a profinite set is Hausdorff and totally disconnected.

Let now X be a compact, Hausdorff, and totally disconnected topological group. Let Ω be the set of open subsets of X. Let $\mathcal{F}$ be the set of finite subsets F of Ω such that $X = \coprod_{U \in F} U$. We order $\mathcal{F}$ by setting $F \leq F'$ if each element of F' is contained in some element of F. In this case we have a map of finite discrete spaces $F' \to F$.

(ii) Show that the elements $F \in \mathcal{F}$ form an inverse system (indexed by $\mathcal{F}$), and that its inverse limit Y is profinite. Show that there is a natural continuous map $f: X \to Y$.

(iii) Show that f is injective.
(iv) Show that the image of f is dense.
(v) Conclude that $f\colon X \to Y$ is a homeomorphism.

GALOIS COHOMOLOGY
EXERCISES 8 (ÉTALE ALGEBRAS)

Let k be a field.

Exercise 1. Let A be an étale k-algebra. Recall that $\mathbf{X}(A)$ denotes the set k-algebra morphisms $A \to k_s$, where k_s is a separable closure of k.

(i) Let B be a quotient algebra of A. Show that B is étale and that the map $\mathbf{X}(B) \to \mathbf{X}(A)$ is injective.
(ii) Let B be a subalgebra of A. Show that B is étale and that the map $\mathbf{X}(A) \to \mathbf{X}(B)$ is surjective. (Hint: assuming that the map is not surjective, produce an element of the kernel of $\mathbf{M}(\mathbf{X}(A)) \to \mathbf{M}(\mathbf{X}(B)$.)
(iii) Show that A has only finitely many subalgebras and quotient algebras.
(iv) Assume that k is infinite. Show that there exists a separable polynomial P such that $A \simeq k[X]/P$. (Hint: to show that A is generated by a single element as a k-algebra, observe that no k-vector space is a finite union of proper subspaces.)

Exercise 2. Let A be a finite-dimensional k-algebra. For an element $a \in A$ recall that $\mathrm{Tr}_{A/k}(a) \in k$ as the trace of the k-linear map $A \to A$ given by $x \mapsto ax$.

(i) Show that a k-algebra A is étale if and only if for every nonzero $a \in A$ there exists $b \in A$ such that $\mathrm{Tr}_{A/k}(ab) \neq 0$.
(ii) Show that a finite field extension L/k is separable if and only if the map $\mathrm{Tr}_{L/k} \colon L \to k$ is nonzero.

Exercise 3. Let K/k be a field extension. We have seen that there is at most one group G (up to isomorphism) such that K is a Galois G-algebra (namely K/k must be Galois, and $G = \mathrm{Gal}(K/k)$). We give here an example of an algebra A admitting G-Galois structures for nonisomorphic group G.

Let K be a separable quadratic extension of k, and $A = K \times K$.

(i) Define a $\mathbb{Z}/4$-Galois algebra structure on A.
(ii) Define a $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$-Galois algebra structure on A.

GALOIS COHOMOLOGY
EXERCISES 9 (TORSORS)

Let k be a field.

Exercise 1. Let k_s be a separable closure of k, and $\Gamma = \mathrm{Gal}(k_s/k)$. Let A be an étale k-algebra of dimension n. Consider the associated Γ-set $X = \mathrm{Hom}_{k-\mathrm{alg}}(A, k_s)$. Let $Y \subset X^n$ be the set of those $(x_1, \ldots, x_n)$ such that $x_i \neq x_j$ when $i \neq j$, with the Γ-action given by

$$\gamma(x_1, \ldots, x_n) = (\gamma x_1, \ldots, \gamma x_n) \quad \text{for } \gamma \in \Gamma, \text{ and } x_1, \ldots, x_n \in X.$$

The symmetric group $\mathfrak{S}_n$ acts on Y by

$$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Denote by Z the quotient of Y be the action of the subgroup $\mathfrak{A}_n$ of even permutations (the kernel of the signature morphism $\mathfrak{S}_n \to \mathbb{Z}/2$).

(i) Show that Z is a Γ-set having two elements.

We denote by Δ the corresponding étale k-algebra of dimension two; it is called the *discriminant algebra* of A.

Assume that k has characteristic $\neq 2$. Let $e_1, \ldots, e_n$ be a k-basis of A, let $f_1, \ldots, f_n$ be the elements of X, and consider the matrix $M = (f_i(e_j)) \in M_n(k_s)$. Set $u = \det M \in k_s$. Let Γ_0 be the subgroup of Γ consisting of those elements acting by even permutations on the set X.

(ii) Let $\gamma \in \Gamma$. Show that $\gamma u = u$ if $\gamma \in \Gamma_0$ and $\gamma u = -u$ otherwise.

Let d be the determinant of the matrix $(\mathrm{Tr}_{A/k}(e_i e_j)) \in M_n(k)$.

(iii) Show that $d = u^2$. (Hint: compute the product $M^t \cdot M$.)
(iv) Conclude that $\Delta = k[X]/(X^2 - d)$.

Exercise 2. Let G be a finite group. Let $H \subset G$ be a subgroup and B a H-algebra over k. Consider the set

$$\mathrm{Ind}_H^G B = \{\text{maps } f\colon G \to B \text{ such that } f(h \cdot g) = h \cdot f(g) \text{ for all } g \in G, h \in H\},$$

viewed as a k-algebra, via pointwise operations on B.

(i) Show that the k-algebra $\mathrm{Ind}_H^G B$ is étale if and only if B is étale

If $f \in \mathrm{Ind}_H^G B$ and $g \in G$, we define an element $g \cdot f \in \mathrm{Ind}_H^G B$ by mapping a $x \in G$ to $f(x \cdot g)$. This gives $\mathrm{Ind}_H^G B$ the structure of a G-algebra.

(ii) Show that the H-algebra B is Galois over k if and only if the G-algebra $\mathrm{Ind}_H^G B$ is Galois over k.
(iii) Let A be a Galois G-algebra over k. Show that there exists a subfield $L \subset A$, which is Galois field extension of k, a subgroup $H \subset G$ isomorphic to $\mathrm{Gal}(L/k)$, and an isomorphism of G-algebras $A \simeq \mathrm{Ind}_H^G L$.

Exercise 3. Let Γ be a profinite group, and $A \to B$ be a morphism of Γ-groups. Describe the map $H^1(\Gamma, A) \to H^1(\Gamma, B)$ in terms of torsors (as opposed to 1-cocyles)

GALOIS COHOMOLOGY
EXERCISES 10 (TWISTED FORMS)

The letter k denotes a field.

Exercise 1. (i) Let V be a k-vector space of finite dimension n, and $f\colon V \times V \to k$ be a k-bilinear form. We assume that $f(x,x) = 0$ for all $x \in V$ (i.e. f is alternated) and that the k-linear map $V \to \operatorname{Hom}_k(V,k)$ sending x to the map $y \mapsto f(x,y)$ is bijective (i.e. f is nondegenerate). Show that n is even, and that V admits a k-basis $e_1, \ldots, e_n$ such that $f(e_{2r+1}, e_{2r+2}) = 1$ and $f(e_{2r+2}, e_{2r+1}) = -1$ for all $0 \leq r < n/2$, and $f(e_i, e_j) = 0$ for all other values of i, j.

(ii) When L/k is a separable field extension, consider the matrix (where blank entries are zero)

$$J = \begin{pmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & -1 & 0 \end{pmatrix} \in M_{2r}(L).$$

Show that letting

$$\operatorname{Sp}_{2r}(L) = \{M \in M_{2r}(L) | M^t J M = J\},$$

where M^t denotes the transpose of M, defines a k-group Sp_{2r} such that $H^1(k, \operatorname{Sp}_{2r}) = \{*\}$.

Exercise 2. For every separable extension L/k set

$$G(L) = \operatorname{Aut}_{L-\mathrm{alg}}(L[X]).$$

Extension of scalars yields a map $G(L) \to G(L')$ for every morphism $L \to L'$ of separable extensions of k.

(i) Show that G defines a k-group. (Caution: As $\dim_k k[X] = \infty$, some of the results of the lectures on twisted forms do not apply directly.)

(ii) Show that every element of $G(L)$ is of the form $X \mapsto aX + b$, where $a \in L^\times$ and $b \in L$.

(iii) Show that we have an exact sequence of k-groups

$$1 \to \mathbb{G}_a \to G \to \mathbb{G}_m \to 1.$$

(iv) Show that $H^1(k, G) = \{*\}$.

Let A be a k-algebra such that $A_L \simeq L[X]$ as L-algebra, for some separable extension L/k.

(v) For every separable extension L/k, consider the set $I(L)$ of isomorphisms of L-algebras $L[X] \to A_L$. Extension of scalars yields a map $I(L) \to I(L')$ for every morphism $L \to L'$ of separable extensions of k. Show that I defines a G-torsor.

(vi) Conclude that $A \simeq k[X]$ as k-algebra.

We now assume that k has positive characteristic p, and that $a \in k$ is such that $a \neq b^p$ for all $b \in k$. We consider the k-algebra $B = k[U,V]/(U^p - aV^p - V)$.

(vii) Show that there exists an algebraic field extension K/k such that $B_K \simeq K[X]$ as K-algebra.

(viii) Show that B is not isomorphic to $k[X]$ as k-algebra. (Hint: If $\varphi\colon B \to k[X]$ is a morphism of k-algebras, consider the equation satisfied by the polynomials $\varphi(U)$ and $\varphi(V)$ to deduce that $\varphi(B) = k$.)

(ix) Give an example of a field k of characteristic p, together with an element $a \in k$ such that $a \neq b^p$ for all $b \in k$.

GALOIS COHOMOLOGY
EXERCISES 11 (CYCLIC ALGEBRAS)

Let k be a field. A finite-dimensional central simple k-algebra A of degree n is called *cyclic* if there exists a Galois $\mathbb{Z}/n$-algebra L and $a \in k^{\times}$ such that A is isomorphic to the cyclic algebra (L, a). The purpose of these exercises is to prove that every central simple algebra of degree 2 or 3 is cyclic (on the other hand one may construct central simple algebras of degree 4 which are not cyclic).

Exercise 1. We have seen that central simple k-algebra of degree 2 are cyclic (in fact quaternion algebras) when k has characteristic $\neq 2$. In this exercise, we consider the case when the characteristic of k is arbitrary.

(i) Let D be a finite-dimensional central simple k-algebra of degree 2. Show that D contains a Galois $\mathbb{Z}/2$-algebra as a k-subalgebra, and deduce that D is cyclic.

(ii) Conclude that every finite-dimensional central simple k-algebra of degree 2 is cyclic.

Exercise 2. Let A be a finite-dimensional central simple k-algebra.

(i) Show that the map

$$\nu \colon A \times A \to k \quad ; \quad (a, b) \mapsto \operatorname{Trd}_A(ab)$$

is a symmetric k-bilinear form.

(ii) Show that the form ν is nondegenerate, i.e. that the set

$$\{a \in A | \operatorname{Trd}_A(ax) = 0 \text{ for all } x \in A\}$$

is reduced to $\{0\}$. (Hint: Show that above set is a two-sided ideal of A.)

Exercise 3. Let A be a finite-dimensional central simple k-algebra of degree n. Let $x \in A$ and $P = \operatorname{Cprd}_A(x) \in k[X]$ its reduced characteristic polynomial.

(i) Show that $P(x) = 0 \in A$.

(ii) Assume that $x \in A^{\times}$, and let $Q = \operatorname{Cprd}_A(x^{-1}) \in k[X]$. Show that

$$P(X) = (-X)^n \cdot \operatorname{Nrd}_A(x) \cdot Q(X^{-1}) \in k[X] \subset k[X, X^{-1}].$$

Exercise 4. Let D be a finite-dimensional central simple division k-algebra of degree 3. When $E \subset D$ is a subset, we write

$$E^{\perp} = \{x \in D | \operatorname{Trd}_D(ex) = 0 \text{ for all } e \in E\}.$$

(i) If $V \subset D$ is a k-subspace, show that $\dim_k V^{\perp} = 9 - \dim_k V$. (Hint: Use Exercise 2.)

(ii) Let K be a commutative k-subalgebra of D. Show that $K = k$ or that K/k is a field extension of degree 3.

(iii) Let $x \in D^\times$ be such that $\mathrm{Trd}_D(x) = \mathrm{Trd}_D(x^{-1}) = 0$. Show that $x^3 = \mathrm{Nrd}_D(x) \in k \subset D$. (Hint: Use Exercise 3.)

(iv) Let $E \subset D$ be a maximal subfield. Find $z \in D - k$ such that $\mathrm{Trd}_D(z) = \mathrm{Trd}_D(z^{-1}) = 0$. (Hint: Pick a nonzero element $u_1 \in E^\perp$, and find $u_2 \in \{u_1^{-1}\}^\perp \cap E$ such that $u_2 \notin u_1 k$. Set $z = u_1 u_2^{-1}$.)

(v) Let F be the k-subalgebra of D generated by z. Find $y \in D - F$ such that

$$\mathrm{Trd}_D(yz) = \mathrm{Trd}_D(yz^2) = \mathrm{Trd}_D(z^{-1}y^{-1}) = \mathrm{Trd}_D(z^{-2}y^{-1}) = 0.$$

(Hint: Pick $v_1 \in F^\perp - F$. Let $V = \{z^{-1}, z^{-2}\}^\perp$, and find a nonzero $v_2 \in (v_1 V) \cap F$. Set $y = v_2^{-1} v_1$.)

(vi) Let L be the k-subalgebra of D generated by y. Show that zyz^{-1} commutes with y and deduce that $zyz^{-1} \in L$. (Hint: Show that $\mathrm{Nrd}_D(yz^2)\,\mathrm{Nrd}_D(z^{-1}) = \mathrm{Nrd}_D(yz)$, and expand using (iii).)

(vii) Show that $y \mapsto zyz^{-1}$ defines a structure of Galois $\mathbb{Z}/3$-algebra on L.

(viii) Deduce that $D \simeq (L, \mathrm{Nrd}_D(z))$.

(ix) Conclude that every finite-dimensional central simple k-algebra of degree 3 is cyclic (this is a theorem of Wedderburn).

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 $\overline{k} \simeq k[X]/(X^2 + 1)$.