Théorie des nombres - TD2

Exercise 1 (A practical example)**.** Let $A =< x, y >=: k\{x, y\} \subset M_2(k)$ [1] be the subalgebra generated by

$$x = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 2 & \\ 1 & 2 \end{pmatrix}$$

Show that $V = k^2$ is a simple A-module, but not a semi-simple $k[x]$ or $k[y]$-module.

Exercise 2 (Conics and quaternion algebras)**.** Let k be a field and $(a, b) = (a, b)_k$ the quaternion algebra with parameters $a, b \in k^\times$. We denote by $C(a, b)$ the conic of $\mathbb{P}^2_k$ with equation

$$C(a, b) : ax^2 + by^2 = z^2.$$

1. What is the conic of $M_2(k)$?
2. Show that $C(a, b)$ is isomorphic over k to the conic with equation
$$ax^2 + by^2 - abz^2 = 0.$$
3. Deduce that $C(a, b)$ up to k-isomorphism is independent of the choice of the presentation of $(a, b)_k$. *Hint : Call a pure quaternion $q \in (a, b)_k$ if $q^2 \in k$ but $q \notin k$. To what condition $q = x + yi + zj + tk$ is a pure quaternion ?*
4. Show that $(a, b)_k$ is split if and only if $C(a, b)$ has a k-rational point (in $\mathbb{P}^2(k)$).
5. Deduce that $(a, b)_k \simeq M_2(k)$ if k is a finite field (without using $\mathrm{Br}(k) = \{0\}$).
6. Show that if $a \neq 0, 1$, then $(a, 1 - a)_k \simeq M_2(k)$.
7. Show that (a, b) is split over k if and only if (a, b) is split over $k(t)$. Can you interpret this result geometrically ?

Exercise 3 (A condition for splitting)**.** 1. (Rieffel's Lemma) Let A/k a simple algebra, and I be a non-zero (left) ideal. Show that, if $D = \mathrm{End}_A(I)$,
$$\lambda : \begin{array}{ccc} A & \longrightarrow & \mathrm{End}_D(I) \\ a & \longmapsto & (i \mapsto ai) \end{array}$$
is an isomorphism.

2. Let A/k be a central simple algebra. Show that $A \simeq M_n(k)$ if and only if A contains a sub-algebra isomorphic to k^n.

Exercise 4 (Structure of finite type module over simple algebra)**.** Let A/k be a simple k-algebra of finite k-dimension.

1. Show that a finite type A-module is semi-simple.
2. Show that two finite type A-modules are isomorphic if and only if they have the same (finite) dimension over k.
3. Give an example of A a ring, and M a finite type A-module that is not semi-simple.

1. This algebra isn't commutative (justify it), the notation $k\{x, y\}$, as opposed to $k[x, y]$ is here to emphasize this.

Exercise 5 (Polynomial solutions in a division algebra)**.** Let D/k be a central, finite dimensionnal, division algebra. Let $P(t) = t^2 + at + b$ be an irreducible polynomial in $k[t]$.

1. Show that P might have an infinite number of solutions in D *Hint : Try with* $\mathbb{H}/\mathbb{R}$ *and the most obvious irreducible polynomial over* $\mathbb{R}$.
2. Show that if $x \in D$ is a root of P, then y is a root of P if an only if x, y are conjugate in D.

Remark 0.1. This is a particular case of a theorem of Dickson, which states the following :

Theorem 0.2 (Dickson). *Let D be a division ring with center k and $P(t) \in k[t]$ and irreducible polynomial. Then any two roots of P in D are conjugate to each other.*

Exercise 6 (The Brauer group of $\mathbb{Q}$)**.** The goal is to prove that the Brauer group $\mathrm{Br}(\mathbb{Q})$ is not finitely generated.

1. Show that we can find a sequence of primes $p_1, p_2, \ldots, p_n, \ldots$ two by two distincts, and a sequence of integers $a_1, a_2, \ldots, a_n, \ldots$ such that a_i is not a square modulo p_i and $a_i \equiv 1 \pmod{p_j}$ for all $1 \leq j < i$.
2. Show that for all i, $(a_i, p_i)_{\mathbb{Q}}$ is a non-split quaternion algebra and that these algebra are two by two distincts.
3. Show that $\mathrm{Br}(\mathbb{Q})$ is not finitely generated. Can you find an abelian group G that is not finitely generated by such that $G[2]$ is finite non trivial ?

Exercise 7 (Kummer Theory)**.** Our goal is to prove the following statement, known as Kummer Theory.

Theorem 0.3 (Kummer)**.** *Let K be a field, $n \in \mathbb{N}_{\geq 2}$, coprime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$. Assume that $\zeta_n \in K$ for ζ_n a primitive n-th root of 1. Let L be a cyclic extension of K of degree n, then there exists $a \in K$, $\sqrt[n]{a} \in L$ (any element such that $(\sqrt[n]{a})^n = a$) such that $L = K(\sqrt[n]{a})$.*

1. If n, K are as in the statement, and $\sqrt[n]{a} \in \overline{K}$ show that $L = K(\sqrt[n]{a})$ is a (Galois) $\mathbb{Z}/n\mathbb{Z}$-extension of K if for all $r|\ n, r \neq n$, $\sqrt[n]{a}^r \notin K$.
2. Show that if $p = \mathrm{char}(K)$, $a \in K$ and $b \in \overline{K}$ such that $b^p = a$, then $K(b)/K$ is not a Galois extension if $b \notin K$.
3. Suppose $p = \mathrm{char}(K) \neq 0$ and $P \in K[X]$ is an irreducible polynomial of degree n, coprime to p. Then if L is the extension of K given by P, or the splitting field of P then show that L/K is separable.
4. Let L/K be a $\mathbb{Z}/n\mathbb{Z}$-extension, and let $\sigma \in \mathrm{Gal}(L/K)$ a fixed generator. Show that we can find $x \in L$ such that
$$\alpha = x + \zeta_n \sigma^{-1}(x) + \zeta_n^2 \sigma^{-2}(x) + \cdots + \zeta_n^{n-1} \sigma^{1-n}(x) \neq 0.$$
5. Show that L is of the form $K(\sqrt[n]{a})$ for some $a \in K$. *Hint : calculate* $\sigma(\alpha)$.
Additional questions :
6. Fix a separable closure K^{sep}. Denote $K(n)$ the composite of all abelian extension of exponent $e|n$ in K^{sep}. Show that we have a well defined continuous pairing
$$\begin{array}{ccc} K^\times/(K^\times)^n \times \mathrm{Gal}(K(n)/K) & \longrightarrow & \mu_n(K^{sep}) \\ (a, \sigma) & \mapsto & \sigma(\sqrt[n]{a})/\sqrt[n]{a} \end{array}$$
7. Show that this pairing is non-degenerate, i.e. $K^\times/(K^\times)^n \simeq \mathrm{Hom}_{cont}(\mathrm{Gal}(K^{sep}/K), \mu_n)$.
8. Show that there is a bijection
$$\begin{array}{ccc} \{\text{extensions } K \subset L \subset K^{sep}, L/K \text{ abelian , of exponent } e|n\} & \longrightarrow & \{\text{ subgroups } (K^\times)^n \subset \Delta \subset K^\times\} \\ L & \longmapsto & (L^\times)^n \cap K^\times \\ K(\sqrt[n]{\Delta}) & \longleftarrow & \Delta \end{array}$$
where $\sqrt[n]{\Delta} = \{x \in K^{sep}|\ x^n \in \Delta\}$.

Exercise 8 (Another presentation of cyclic algebra)**.** Let k be a field, $n \geq 2$ an integer, coprime to $\mathrm{char}(k)$ if $\mathrm{char}(k) \neq 0$. Suppose that k contains all n-roots of 1, and fix w a primitive n-root of 1. We define the algebra

$$(a, b)_w := k\{x, y\}/(x^n - a, y^n - b, xy = wyx).$$

1. For $n = 2$ show that we obtain exactly quaternion algebras.
2. Justify that if A is a cyclic algebra, for $L/k, \sigma \in \mathrm{Gal}(L/k) \simeq \mathbb{Z}/n\mathbb{Z}, a \in k^\times$, then

   $$A := (\sigma, a) \simeq (a, b)_w,$$

   for some b, w.
3. Show that $(a, b)_w$ is central simple.
4. Prove the following isomorphisms

$$(a, 1)_w \simeq (1, b)_w \simeq M_n(k),$$

$$(a, t^n b)_w \simeq (a, b)_w,$$

$$(a, b)_w \otimes_k (a', b)_w \simeq (aa', b)_w \otimes_k M_n(k).$$

Exercise 9. Let G be a profinite group, V a complex representation and $\rho : G \longrightarrow \mathrm{GL}(V)$ a continuous representation. Show that ρ has finite image.