Math 223a: Algebraic Number Theory

Fall 2019

Homework #11

due Tuesday, November 26 at noon

Problem 1. Let D be any division K-algebra of degree $n = \dim_K(D)$. Let $\mathrm{End}_K(D) \cong M_n(K)$ be the K-algebra of K-vector space endomorphisms of D. Verify that the following defines an isomorphism of K-algebras, so D^{opp} is indeed the inverse of D in the Brauer group $\mathrm{Br}(K)$:

$$\begin{aligned} D \otimes_K D^{\mathrm{opp}} &\longrightarrow \mathrm{End}_K(D) \\ x \otimes y &\longmapsto (t \mapsto xty) \end{aligned}$$

Definition. For a field K of characteristic $\mathrm{char}(K) \neq 2$ and elements $r, s \in K^\times$, define the *Quaternion algebra* $(r,s)_K$ as the four-dimensional K-algebra with basis $1, i, j, k$ and multiplication given by $i^2 = r$, $j^2 = s$, $ij = -ji = k$.

$\cdot$	i	j	k
i	r	k	rj
j	$-k$	s	$-si$
k	$-rj$	si	$-rs$

For example, $(-1,-1)_{\mathbb{R}}$ is the ring $\mathbb{H}$ of Hamilton quaternions. You can show that $(r,s)_K$ is a central simple K-algebra, so it must be isomorphic to $M_n(D)$ for some $n \geqslant 1$ and some central division K-algebra.

Problem 2. Show that $(r,s)_K \otimes_K (r,s)_K \cong M_2(K)$ for all K, r, s as above. (So $(r,s)_K$ has order dividing 2 in $\mathrm{Br}(K)$.)

Problem 3. Let $A = (r,s)_K$ and $t = a + bi + cj + dk \in A$.

a) What is the minimal polynomial of t?

b) Show that $N_{A|K}(t) = (a^2 - rb^2 - sc^2 + rsd^2)^2$.

Problem 4. Show that $A = (r,s)_K$ is a division ring if and only if the equation $a^2 = rb^2 + sc^2$ has no solution $(0,0,0) \neq (a,b,c) \in K^3$.

Problem 5. Using Wedderburn's Theorem, show that for any odd prime p and any $r, s \in \mathbb{F}_p^\times$ the equation $a^2 - rb^2 - sc^2 + rsd^2 = 0$ has exactly $p^3 + p^2 - p$ solutions $(a, b, c, d) \in \mathbb{F}_p^4$.

Definition. Let D be a division $\mathbb{Q}$-algebra. An element x of D is called *integral* if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$. In the noncommutative case, it generally doesn't make sense to talk about *the ring of integers*. Instead, one looks at *maximal orders*:

Problem 6. Consider the ring R of elements $a + bi + cj + dk$ of $\mathbb{H}$ such that a, b, c, d are either all integers (elements of $\mathbb{Z}$) or all half-integers (elements of $\frac{1}{2} + \mathbb{Z}$).

a) Show that every element of R is integral.

b) Show that R doesn't contain all integral elements of $\mathbb{H}$.

c) Show that there is no larger subring $R' \supsetneq R$ of $\mathbb{H}$ that contains only integral elements.

d) Show that the unit group $R^\times$ consist of exactly the following 24 elements: $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$