# Math 80220 Algebraic Number Theory
# Problem Set 8

Andrei Jorza

Optional

1. Let $K$ be a field. A polynomial $f \in K[X]$ is said to be *additive* if $f(X+Y) = f(X) + f(Y)$ is satisfied in $K[X,Y]$.

   (a) If $K$ has characteristic 0 show that the additive polynomials are the polynomials $f(X) = aX$ for some $a \in K$.

   (b) If $K$ has characteristic $p > 0$ show that the additive polynomials are the polynomials

   $$f(X) = a_0 X + a_1 X^p + a_2 X^{p^2} + \cdots a_n X^{p^n}$$

   [Hint: Show that $f'(X)$ is constant.]

2. Let $p$ be a prime and $q = p^r$ and let $K = \mathbb{F}_q(T)$ and let $\mathcal{O} = \mathbb{F}_q[T]$. Write $\mathcal{A}(K)$ for the set of additive polynomials. Let $\phi(x) = x^q$ be Frobenius in $K$ and let $K\langle\phi\rangle$ be the set of polynomial expressions in $\phi$ (i.e., $a_0 + a_1\phi + \cdots a_k\phi^k$) with usual addition and the unique noncommutative multiplication characterized by $\phi a = a^q \phi$ and usual multiplication of scalars.

   (a) Show that the map $\Psi : \mathcal{A}(K) \to K\langle\phi\rangle$ given by $\sum_{i=0}^n a_i X^{p^i} \mapsto \sum_{i=0}^n a_i \phi^i$ satisfies $\Psi(f \circ g) = \Psi(f)\Psi(g)$ and yields an isomorphism of (noncommutative) rings.

   (b) A *Drinfel'd module* is a ring homomorphism $\rho : \mathcal{O} \to K\langle\phi\rangle$ such that for every polynomial $P(T)$, $\rho(P(T))$ has constant term $P(T)$ and $\operatorname{Im}\rho \not\subset K$. Show that for any polynomial $f \in K\langle\phi\rangle$ of degree $r$ and with constant term 0 there exists a Drinfel'd module $\rho : \mathcal{O} \to K\langle\phi\rangle$ such that

   $$\rho(T) := T + f(\phi)$$

   Such a Drinfel'd module is said to have *rank* $r = \deg f$.

   (c) Let $\rho : \mathcal{O} \to K\langle\phi\rangle$ be a rank 1 Drinfel'd module. Consider the $\mathcal{O}$-module $\overline{K}_\rho$ whose underlying set is $\overline{K}$ but with multiplication given by $a \cdot u := \rho(a,u)$ where the polynomial $\rho(a) = f(\phi)$ acts on $u \in \overline{K}$ as

   $$\rho(a,u) = f(\phi)(u)$$

   via $\phi(u) = u^q$.

   i. Show that indeed $\overline{K}_a$ is an $\mathcal{O}$-module.

   ii. Show that the set $\overline{K}_\rho[a] := \{u \in \overline{K}_\rho | a \cdot u = 0\}$ is an $\mathcal{O}$-module.

   iii. Show that if $a \in \mathcal{O}$ is a polynomial of degree $d = \deg a$ and $u \in \overline{K}_\rho$ then

   $$\rho(a,u) = au + \sum_{i=1}^{d} b_i u^{q^i}$$

   with $b_d \neq 0$ and $b_i \in K$ depend on $a$ but not on $u$.

iv. Conclude the $\overline{K}_\rho[a]$ has $q^{\deg a}$ elements. [Hint: Recall that $a \cdot u = \rho(a, u)$ and show that this polynomial is separable.]

v. Show that as $\mathcal{O} = \mathbb{F}_q[T]$-modules we have $\overline{K}_\rho[a] \cong \mathcal{O}/(a)$. [Hint: $\mathcal{O}$ is a PID and count the cardinality of $\mathcal{O}/(a)$.]

(d) Let $\rho$ be a rank 1 Drinfel'd module and $a \in \mathbb{F}_q[T]$. Let $K_a$ be the splitting field of the polynomial $\rho(a, X)$, i.e., the finite extension of $K$ generated by the $q^{\deg a}$ elements of $\overline{K}_\rho[a] \subset \overline{K}$. Show that $K_a/K$ is a finite Galois extension with Galois group

$$\mathrm{Gal}(K_a/K) \subset \mathrm{Aut}(\overline{K}_\rho[a]) \cong (\mathcal{O}/(a))^\times$$

[Hint: The Galois group permutes roots of polynomials.]

3. The *Carlitz module* is the Drinfel'd module $\rho : \mathcal{O} \to K\langle\phi\rangle$ with $\rho(T) = T + \phi$. From the previous exercise we know that for $a \in \mathbb{F}_q[T]$ the Galois group $\mathrm{Gal}(K_a/K)$ is a subgroup of $(\mathcal{O}/(a))^\times$. The goal of this exercise is to show that in fact $\mathrm{Gal}(K_a/K) \cong (\mathcal{O}/(a))^\times$ (which we used to study irreducible polynomials in $\mathbb{F}_q[T]$ in arithmetic progressions).

(a) Suppose $a \in \mathbb{F}_q[T]$ has degree $d$ and let $\zeta_a \in \overline{K}_\rho[a]$ whose image in $\mathcal{O}/(a)$ is a generator of the $\mathcal{O}$-module $\mathcal{O}/(a)$. Show that via the isomorphism $\overline{K}_\rho[a] \cong \mathcal{O}/(a)$ for $b \in \mathbb{F}_q[T]$ the element $b \cdot \zeta_a = \rho(b, \zeta_a)$ generates $\mathcal{O}/(a)$ if and only if $(a, b) = 1$.

(b) Deduce that $K_a = K(\zeta_a)$ and that the number of such generators is $\varphi(a) := |(\mathcal{O}/(a))^\times|$. [Hint: The previous part shows that the elements of $\overline{K}_\rho[a]$ are of the form $\rho(b, \zeta_a)$.]

(c) Let $a, b \in \mathcal{O}$ coprime at let $\mathcal{O}_a$ be the integral closure of $\mathcal{O}$ in the field $K_a$. Show that $\zeta_a \in \mathcal{O}_a$ (this is where you use that $\rho(T) = T + \phi$) and that $\frac{b \cdot \zeta_a}{\zeta_a}$ is a unit in $\mathcal{O}_a^\times$. [Hint: Use the formula for $b \cdot \zeta_a$ and the fact that if $cb \equiv 1 \pmod{a}$ then $c \cdot (b \cdot \zeta_a) = \zeta_a$.]

(d) Show that $\mathcal{O}$ and $\mathcal{O}_a$ are Dedekind domains. [Hint: For the first one show directly. For the second one you may use the fact that the integral closure of a Dedekind domain in a finite extension of its fraction field is again a Dedekind domain.]

(e) Suppose $a = P^e \in \mathcal{O}$ where $P$ is an irreducible polynomial in $\mathcal{O} = \mathbb{F}_q[T]$.

i. Show that the polynomial

$$\Phi_a(u) = \prod_{b \in (\mathcal{O}/(a))^\times} (u - b \cdot \zeta_a) \in \mathcal{O}[u]$$

is equal to

$$\Phi_{P^e}(u) = \frac{P^e \cdot u}{P^{e-1} \cdot u}$$

[Hint: Show that the RHS is a polynomial of the same degree as the LHS and having as roots all the distinct roots of the LHS.]

ii. Conclude that $\displaystyle\prod_{(b,P)=1, \deg(b) < e \deg(P)} b \cdot \zeta_a = P$. [Hint: What is $\Phi_{P^e}(0)$?]

iii. Show that the ideal $(P)\mathcal{O}_a$ is equal to the ideal $(\zeta_a)^{\varphi(P^e)}$. [Hint: $b \cdot \zeta_a$ and $\zeta_a$ differ by a unit in $\mathcal{O}_a^\times$.]

iv. Conclude that $[K_{P^e} : K] \geq \varphi(P^e)$ and thus that $\mathrm{Gal}(K_{P^e}/K) \cong (\mathcal{O}/P^e)^\times$ and that $P$ is totally ramified in $\mathcal{O}_a$. [Hint: In a Dedekind domain the ramification index is at most equal to the degree of the extension of fraction fields.]

v. Let $f(u)$ be the minimal polynomial over $K$ of $\zeta_a$. Show that $P^e \cdot u = f(u)g(u)$ for some $g \in \mathcal{O}[u]$ and that $P^e = f'(\zeta_a)g(\zeta_a)$. [Hint: Look at the lowest degree monomials.]

vi. Recall that $\zeta_a \in \mathcal{O}_a$. Show that $f'(\zeta_a) \in \mathcal{D}_{\mathcal{O}_a/\mathcal{O}}$ where $\mathcal{D}_{\mathcal{O}_a/\mathcal{O}}$ is the different ($\mathcal{D}^{-1}_{\mathcal{O}_a/\mathcal{O}} = \{x \in \mathcal{O}_a | \operatorname{Tr}_{K_a/K}(x\mathcal{O}_a) \subset \mathcal{O}\}$). (In fact this is true for any extension of Dedekind domains.) [Hint: Show that the dual basis to $1, \zeta_a, \ldots, \zeta_a^{d-1}$ with respect to the trace pairing is given by the coefficients of the polynomial $\dfrac{f(u)}{(u-\zeta_a)f'(\zeta_a)}$.]

vii. Deduce that every prime ideal in the different must divide $P$ and thus that if $Q \in \mathcal{O}$ is an irreducible polynomial coprime to $P$ then $Q$ is unramified in $\mathcal{O}_a$. [Hint: Recall that the ramified primes are the primes dividing the different.]

(f) Now suppose that $a = \alpha P_1^{e_1} \cdots P_r^{e_r}$ is the factorization of $a$ into irreducibles, where $\alpha \in \mathbb{F}_q^\times$.

i. Write $a_i = a/P_i^{e_i}$. Show that $\zeta_{P_i^{e_i}} := a_i \cdot \zeta_a$ is a generator of $\overline{K}_\rho[P_i^{e_i}]$.

ii. Show that $K_a$ contains each $K_{P_i^{e_i}}$ and thus the compositum of these fields.

iii. Let $Q_i \in \mathcal{O}$ be such that $\sum P_i Q_i = 1$. Show that $\zeta_a = \sum Q_i \cdot \zeta_{P_i^{e_1}}$ and deduce that $K_a = \prod K_{P_i^{e_i}}$ is the compositum.

iv. Show that $K_{P_1^{e_1}} \cdots K_{P_e^{e_k}}$ ramifies only at primes dividing $P_1, \ldots, P_k$. [Hint: If $A \subset B, C$ are dedekind domains if a prime of $A$ is unramified in $B$ and $C$ then it is unramified in the compositum.]

v. Show that the only extension of $K$ unramified at all primes is $K$ itself.

vi. Show that $K_{P_1^{e_1}} \cdots K_{P_e^{e_k}} \cap K^{e_{k+1}}_{P_{k+1}} = K$.

vii. Deduce that $\operatorname{Gal}(K_a/K) \cong \prod_i (\mathcal{O}/P_i^{e_i})^\times \cong (\mathcal{O}/a)^\times$.