Math 80220 Algebraic Number Theory
The Leftovers

Andrei Jorza

due never

1 Rings of integers

1. The discriminant of a polynomial $f \in K[X]$ with roots $\alpha_1, \ldots, \alpha_n$ is

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j)$$

   (a) Show that the discriminant of $f(X) = X^n + pX + q$ is

$$(-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

   (b) For p an odd prime show that the discriminant of $\mathbb{Q}(\zeta_p)$ is $(-1)^{(p-1)/2} p^{p-2}$ and deduce that $\mathbb{Q}(\zeta_p)$ contains $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$. [Hint: square root of the discriminant is an element of the field!]

2. Let K, L be two number fields and assume that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. In this exercise you study when $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$.

   (a) Suppose α_i is an integral basis of $\mathcal{O}_K$ and β_j is an integral basis of $\mathcal{O}_L$. Show that $\alpha_i \beta_j$ form an integral basis of $\mathcal{O}_K \mathcal{O}_L$. [Hint: what is the degree of KL/L?]

   (b) Show that every $\alpha \in \mathcal{O}_{KL}$ is of the form

$$\alpha = \sum_{i,j} \frac{m_{i,j}}{r} \alpha_i \beta_j$$

   where $r, m_{i,j} \in \mathbb{Z}$ with r coprime to $\gcd(m_{i,j})$.

   (c) Recall that the embeddings of $KL \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$ are of the form $\sigma\tau$ where $\sigma : K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$ and $\tau : KL \hookrightarrow \mathbb{C}$ fixing L.
   Let $x_i = \sum_j \frac{m_{i,j}}{r} \beta_j$ and $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K \hookrightarrow \mathbb{C}$ fixing $\mathbb{Q}$. Show that $\sum_i \sigma_j(\alpha_i) x_i = (\sigma_j \tau)(\alpha)$. If $d = \det((\sigma_j(\alpha_i))$ show that $x_i \in \frac{1}{d}\overline{\mathbb{Z}}$ where $\overline{\mathbb{Z}}$ is the ring of algebraic integers.

   (d) Recall that $d^2 = D = \operatorname{disc}(\mathcal{O}_K) \in \mathbb{Z}$ and show that $Dx_i = \sum \frac{Dm_{i,j}}{r} \beta_j \in \mathcal{O}_L$. Deduce that $r \mid D$ and $r \mid \gcd(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_L))$.

   (e) Conclude that if $\operatorname{disc}(\mathcal{O}_K)$ and $\operatorname{disc}(\mathcal{O}_L)$ are coprime then $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$. In particular, show that if n is square-free then $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. (Recall that we proved this for n prime.)

   (f) Show that $\frac{\sqrt{3}+\sqrt{7}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{7})} - \mathcal{O}_{\mathbb{Q}(\sqrt{3})} \mathcal{O}_{\mathbb{Q}(\sqrt{7})}$.

2 Prime ideals in extensions and ramification

3. Let $L, L'/K$ be number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ which splits completely in L and L'. Suppose $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $\mathfrak{p}$ is coprime to $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.

   (a) Let $f(X)$ be the minimal polynomial of α over K. Show that $f \pmod{\mathfrak{p}}$ splits into linear factors.

   (b) Show that $LL' = L'(\alpha)$ and the minimal polynomial $g(X)$ of α over L divides $f(X)$ in $\mathcal{O}_{L'}[X]$.

   (c) For every prime ideal $\mathfrak{q}' \mid \mathfrak{p}$ of $\mathcal{O}_{L'}$ show that $\mathfrak{q}'\mathcal{O}_{LL'}$ splits completely.

   (d) Deduce that $\mathfrak{p}$ splits completely in the composite extension LL'.

4. For which m, n square-free, $\neq 1$ and coprime is $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}(\sqrt{mn})$ everywhere unramified? You may use the fact that an integral basis of the ring of integers of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is given by

m	n	Integral basis
$\equiv 3 \pmod 4$	$\equiv 3 \pmod 4$	$1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{mn}}{2}$
$\equiv 3 \pmod 4$	$\equiv 2 \pmod 4$	$1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{mn}}{2}$
$\equiv 1 \pmod 4$	$\equiv 2, 3 \pmod 4$	$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{mn}}{2}$
$\equiv 1 \pmod 4$	$\equiv 1 \pmod 4$	$1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{mn}}{4}$

5. (a) Show that the only finite extension of $\mathbb{Q}$ that is everywhere unramified is $\mathbb{Q}$.

   (b) Show that the only finite extension of $\mathbb{Q}(i)$ that is everywhere unramified is $\mathbb{Q}(i)$.

3 Chebotarev density

6. For an integer $n \geq 1$ let $\ell(n)$ be the length of the period of $1/n$ written in decimal notation. For example, $1/2 = 0.5$ so $\ell(2) = 0$, $1/12 = 0.08(3)$ so $\ell(12) = 1$ and $1/675 = 0.00(148)$ so $\ell(675) = 3$. The purpose of this problem is to show that $\ell(p)$ is an odd number for one third of the primes p.

   (a) Show that if $(n, 10) = 1$ then $\ell(n)$ is the order of 10 in $(\mathbb{Z}/n\mathbb{Z})^\times$.

   (b) Let $p \nmid 10$ and $k \geq 1$. Show that p splits completely in $\mathbb{Q}(\zeta_{2^k})$ but not in $\mathbb{Q}(\zeta_{2^{k+1}})$ if $p - 1 = 2^k m$ where m is odd.

   (c) Let $n \geq 2, d \geq 1$ be integers and a be a square-free integer. Show that $K = \mathbb{Q}(\sqrt[n]{a}, \zeta_{nd})$ is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/nd\mathbb{Z})^\times \rtimes \mathbb{Z}/n\mathbb{Z}$.

   (d) Suppose $p = 2^k m$ as above and assume that $X^{2^k} \equiv 10 \pmod p$ has a solution in $\mathbb{F}_p$. Show that p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$. [Hint: What is the minimal polynomial of $\sqrt[2^k]{10}$ over $\mathbb{Q}(\zeta_{2^k})$?]

   (e) Reciprocally, if $p \nmid 10$ and $k \geq 1$ show that p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ implies that 2^k is the largest power of 2 in $p - 1$ and $X^{2^k} \equiv 10 \pmod p$ has a solution in $\mathbb{F}_p$. [Hint: You may use the fact that if p splits completely in K and L then it does so in the composite KL.]

   (f) Deduce that $\ell(p)$ is odd if and only if p splits completely in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})$ but not in $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})$ for some $k \geq 1$.

   (g) Show that $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^k})/\mathbb{Q}$ is Galois of order 2^{2k-1} and $\mathbb{Q}(\sqrt[2^k]{10}, \zeta_{2^{k+1}})/\mathbb{Q}$ is Galois of order 2^{2k}.

   (h) Show that the density of primes p such that $\ell(p)$ is an odd number is $1/3$. [Hint: Recall that splitting completely means trivial Frobenius.]

   For more about this problem see Odoni, "A Conjecture of Krishnamurty on decimal periods and some allied problems". You are more than welcome to try to decipher that paper to figure out a solution for this problem (which is a very special case of that paper).

7. Let $N > 1$ be an integer and $\Phi_N(X)$ be the N-th cyclotomic polynomial, i.e., the minimal polynomial of ζ_N.

   (a) If $p \nmid N$ is a prime show that $\Phi_N(X) \mod p$ factors as a product of irreducible polynomials of the same degree $d \mid \varphi(N)$.

   (b) Let n_d be the number of $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ of order d. Show that the density of primes p such that $\Phi_N \mod p$ factors as a product of polynomials of degree $d \mid \varphi(N)$ equals $\dfrac{n_d}{\varphi(N)}$.

   (c) Write $N = 2^k p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorization of N. If $4 \nmid N$ suppose that $r \geq 2$ and if $4 \mid N$ suppose that $r \geq 1$. Show that the set of primes p which are inert in $\mathbb{Q}(\zeta_N)$ has density 0. [Hint: What is $(\mathbb{Z}/N\mathbb{Z})^\times$ as a product of cyclic groups?]

8. Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial of degree n with Galois group S_n. Suppose

$$n = \underbrace{n_1 + \cdots + n_1}_{m_1} + \cdots + \underbrace{n_k + \cdots n_k}_{m_k}$$

   where $n_1 > \cdots > n_k \geq 1$. Show that the density of primes such that $f \mod p = \prod f_i$ with $(\deg f_i) = (n_1, \ldots, n_1, \ldots, n_k, \ldots, n_k)$ (up to permutation) is

$$\frac{1}{\prod n_i^{m_i} \prod m_i!}$$

9. Take for granted that the number $\pi(x)$ of primes $\leq x$ is $\pi(x) = \dfrac{x}{\log x} + o(\frac{x}{\log x})$. Show that the set of primes that begin with the digit 1 in base 10 does not have natural density.

4 Eisenstein series

10. (a) Show that

$$\pi \operatorname{cotan}(\pi z) = \frac{1}{z} + \sum_{n \geq 1} \left(\frac{1}{z+n} + \frac{1}{z-n} \right)$$

    [Hint: Use the previous exercise.]

    (b) Writing $q = \exp(2\pi i z)$ show that

$$\pi \operatorname{cotan}(\pi z) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n$$

    [Hint: What are $\sin(\pi z)$ and $\cos(\pi z)$ in terms of q?]

    (c) Deduce that for $k \geq 2$

$$\sum_{n \in \mathbb{Z}} \frac{1}{(n+z)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n$$

    [Hint: Differentiate the two expressions for $\pi \operatorname{cotan}(\pi z)$.]

    (d) For $k \geq 1$ consider the expression $G_{2k}(z) = \displaystyle\sum_{(m,n) \neq (0,0), m,n \in \mathbb{Z}} \frac{1}{(mz+n)^{2k}}$. Show that

$$G_{2k}(z) = 2\zeta(2k) + 2 \sum_{m \geq 1, n \in \mathbb{Z}} \frac{1}{(mz+n)^{2k}}$$

and conclude that

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{2k-1}(n)q^n$$

where $\sigma_r(n) = \sum_{d|n} d^r$.

(e) Show that $E_{2k} = \dfrac{(2k-1)!}{2(-2\pi i)^{2k}}G_{2k}$ satisfies

$$E_{2k} = \frac{\zeta(1-2k)}{2} + \sum_{n\geq 1}\sigma_{2k-1}(n)q^n$$

and so is in $\mathbb{Q}[\![q]\!]$.

(f) Show that $E_{12} \equiv \sum_{n\geq 1}\sigma_{11}(n)q^n \pmod{691}$ and thus lies in $q\mathbb{F}_{691}[\![q]\!]$. (You may look up the Bernoulli number B_{12}.)

(g) Show, directly from the definition, that if $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$ then

$$G_{2k}\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k}G_{2k}(z)$$

Remark 1. Part 10g shows that G_{2k} and E_{2k} are *modular forms*. Part 10f implies one of the Ramanujan identities, that if $\tau(n)$ is the coefficient of q^n in $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$ then $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ (one shows that $E_{12} \equiv \Delta \pmod{691}$) because both power series start with $q \pmod{691}$).

5 L-functions

11. Let G be a finite abelian group and $f : G \to \mathbb{C}$ be any function.

(a) Show that the vector space V of functions from G to $\mathbb{C}$ has the following sets as bases:

i. The set $\mathcal{B}_1$ of functions $\phi_g : G \to \mathbb{C}$ as $g \in G$ defined as $\phi_g(h) = \begin{cases} 1 & g = h \\ 0 & g \neq h \end{cases}$.

ii. The set $\mathcal{B}_2$ of characters $\chi \in \widehat{G}$.

(b) Show that the linear transformation $T : V \to V$ defined by $(T\phi)(g) = \sum_{h\in G} f(g)\phi(gh)$ has matrix $(f(gh^{-1})_{g,h\in G}$ with respect to the basis $\mathcal{B}_1$ and is diagonal with respect to the basis $\mathcal{B}_2$ and conclude that

$$\det(f(gh^{-1})_{g,h\in G} = \prod_{\chi\in\widehat{G}}\sum_{g\in G}\chi(g)f(g)$$

(c) Show that the vector subspace $W \subset V$ of functions ϕ such that $\sum_{g\in G}\phi(g) = 0$ has the following sets as bases:

i. The set $\mathcal{B}_1'$ of functions $\psi_g(h) = \phi_g(h) - 1/|G|$.

ii. The set $\mathcal{B}_2'$ of characters $\chi \neq 1$.

(d) Show that the linear transformation T stabilizes W (i.e., $T(W) = W$) and with respect to the basis $\mathcal{B}_1'$ has matrix $(f(gh^{-1}) - f(g))_{g,h\neq 1}$ and is diagonal with respect to $\mathcal{B}_2'$ and deduce that

$$\det(f(gh^{-1}) - f(g))_{g,h\neq 1} = \prod_{\chi\neq 1}\sum_{g\in G}\chi(g)f(g)$$

12. Let $p > 2$ be a prime number and $K = \mathbb{Q}(\zeta_p)$. Recall from the first homework that if $p^* = (-1)^{(p-1)/2}p$ then $\mathbb{Q}(\sqrt{p^*}) \subset K$.

(a) The group $G = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and therefore so is its character group $\widehat{G}$. Denote χ a generator, taking a generator of G to ζ_{p-1}. Show that

$$\chi^{(p-1)/2}(x) = \left(\frac{x}{p}\right)$$

(b) Show that if H is the subgroup of $G \cong \mathbb{Z}/(p-1)\mathbb{Z}$ corresponding to $\{0, 2, 4, \ldots, p-3\} \subset \{0, 1, 2, \ldots, p-2\}$ then the fixed subfield is $K^H = \mathbb{Q}(\sqrt{p^*})$. [Hint: Show that there is only one quadratic subfield of K.]

(c) Show that the characters χ^k and $\chi^{k+(p-1)/2}$ are equal on H and conclude that the characters of $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ are 1 and $\left(\frac{\cdot}{p}\right)$. Deduce that

$$\tau\left(\left(\frac{\cdot}{p}\right)\right) = \sqrt{p^*}$$

[Hint: For the Gauss sum, use the result from class.]

(d) If $p \equiv 3 \pmod 4$ show that

$$L\left(\left(\frac{\cdot}{p}\right), 1\right) = \begin{cases} \dfrac{\pi}{3\sqrt{3}} & p = 3 \\ \dfrac{\pi h_{\mathbb{Q}(\sqrt{-p})}}{\sqrt{p}} & p > 3 \end{cases}$$

and conclude that

$$B_{1,\left(\frac{\cdot}{p}\right)} = \begin{cases} -\dfrac{1}{3} & p = 3 \\ -h_{\mathbb{Q}(\sqrt{-p})} & p > 3 \end{cases}$$

and thus that if $p > 3$ we have

$$h_{\mathbb{Q}(\sqrt{p^*})} = -\frac{1}{p}\sum_{k=1}^{p}\left(\frac{k}{p}\right)k$$

(e) If $p \equiv 1 \pmod 4$ and $a + b\sqrt{p}$ is a generator for the unit group $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{p})} = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]^\times$ show that

$$L\left(\left(\frac{\cdot}{p}\right), 1\right) = \frac{2h_{\mathbb{Q}(\sqrt{p})}|\log|a + b\sqrt{p}||}{\sqrt{p}}$$

and conclude that

$$h_{\mathbb{Q}(\sqrt{p})} = -\frac{1}{2|\log|a + b\sqrt{p}||}\sum_{k=1}^{p}\left(\frac{k}{p}\right)\log|1 - \zeta_p^k|$$

13. Let $K = \mathbb{Q}(\sqrt{3})$ and $\chi : K^\times \to \mathbb{C}^\times$ be $\chi(x) = \mathrm{sign}\, N_{K/\mathbb{Q}}(x)$.

(a) Show that $u \in \mathcal{O}_K^\times$ if and only if $N_{K/\mathbb{Q}}(u) = 1$ (i.e., no -1 can occur). Show that one may choose a generator $u = a + b\sqrt{3}$ of $\mathcal{O}_K^\times$ such that $a, b > 0$. Deduce that $\mathcal{O}_K^\times = \pm(2 + \sqrt{3})^{\mathbb{Z}}$. [Hint: Show that $(a + b\sqrt{3})^k = 2 + \sqrt{3}$ would imply that $a \leq 2$ and $b \leq 1$.

(b) Show that if u is a unit in $\mathcal{O}_K^\times$ then $\chi(xu) = \chi(x)$ and deduce that χ defined a character on the group of ideals of K.

(c) Show that $2\mathcal{O}_K = (1+\sqrt{3})^2$, $3\mathcal{O}_K = (\sqrt{3})^2$ and if $p > 3$ then p splits in $\mathcal{O}_K$ if and only if $\left(\frac{3}{p}\right) = 1$. Show that if p splits with $p = u\overline{u}$ then $\chi(u) = \left(\frac{p}{3}\right)$.

(d) Deduce that

$$L(\chi, s) := \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{||\mathfrak{p}||^s}\right)^{-1} = L\left(\left(\frac{\cdot}{4}\right), s\right) L\left(\left(\frac{\cdot}{3}\right), s\right)$$

[Hint: Use Euler products and decide how a prime of $\mathbb{Q}$ splits in K.]

14. Let F be a number field, S a finite set of prime ideals, and $\zeta_{F,S}(s) = \prod_{\mathfrak{p}\in S}\left(1 - \frac{1}{||\mathfrak{p}||^s}\right)\zeta_F(s)$. We will denote by R_S the S-regulator, i.e., the covolume of $\mathcal{O}_{F,S}^\times$ under the logarithm map $F_\infty \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p} - \{0\} \to \mathbb{R}^{r_1+r_2+|S|-1}$.

(a) Let $\mathfrak{q} \notin S$ be a prime ideal, and denote by m its order in the S-class group $\mathrm{Cl}_S(F)$. Show that

$$m|\,\mathrm{Cl}_{S\cup\{\mathfrak{q}\}}(F)| = |\,\mathrm{Cl}_S(F)|.$$

(b) Show that

$$R_{S\cup\{\mathfrak{q}\}} = m \log ||\mathfrak{q}|| R_S.$$

[Hint: Note that $\mathfrak{q}^m = (\varpi)$ is principal as an ideal of $\mathcal{O}_{F,S}$ and look at the image of ϖ under the logarithm map.]

(c) Conclude that the Taylor expansion of $\zeta_{F,S}(s)$ around 0 is

$$\zeta_{F,S}(s) = -\frac{|(K_0\mathcal{O}_{F,S})_{\mathrm{tor}}|R_S}{|(K_1\mathcal{O}_{F,S})_{\mathrm{tor}}|} s^{\mathrm{rk}\,K_1\mathcal{O}_{F,S}} + O(s^{\mathrm{rk}\,K_1\mathcal{O}_{F,S}+1}).$$

(I got this formulation from Samit Dasgupta's senior thesis.)

15. Let p, q be two primes. This exercises provides a proof of quadratic reciprocity.

(a) Let $\chi(x) = \left(\frac{x}{p}\right)$ a character on $(\mathbb{Z}/p\mathbb{Z})^\times \to \{-1, 1\}$. Recall that the Gauss sum is defined as $\tau(\chi) = \widehat{\chi}(1)$, where $\widehat{\chi}$ is the Fourier transform of χ extended by 0 to a function $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$. Show that $\tau(\chi)^2 = p^* = (-1)^{(p-1)/2}p$. [Hint: What is $|\tau(\chi)|$ and what is $\overline{\tau(\chi)}$?]

(b) Conclude that $\tau(\chi)^q \equiv \tau(\chi)\left(\frac{p^*}{q}\right) \pmod{q\mathbb{Z}[\zeta_q]}$. [Hint: Recall that $\left(\frac{a}{q}\right) \equiv a^{(q-1)/2} \pmod q$.]

(c) Show directly from $\tau(\chi) = \widehat{\chi}(1)$ that $\tau(\chi)^q \equiv \widehat{\chi}(q) \equiv \chi(q)\tau(\chi) \pmod q$.

(d) Deduce that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Cyclotomic theory for polynomials mod p

16. 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

$$f(X) = a_0X + a_1X^p + a_2X^{p^2} + \cdots a_nX^{p^n}$$

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

17. 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 ϕ (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 ρ 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

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

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

18. 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 $\operatorname{Gal}(K_a/K)$ is a subgroup of $(\mathcal{O}/(a))^\times$. The goal of this exercise is to show that in fact $\operatorname{Gal}(K_a/K) \cong (\mathcal{O}/(a))^\times$ (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 $\prod_{(b,P)=1, \deg(b) < e \deg(P)} b \cdot \zeta_a = P$. [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 ζ_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 ζ_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 $\frac{f(u)}{(u - \zeta_a)f'(\zeta_a)}$.]

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

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