CTNT - Summer 2018
Mini-Course C: Function field arithmetic
Exercises

Lecture 1 :

1. We will play with the finite field $\mathbb{F}_{p^r}$ for $p = 3$ and $r = 2$.
   (a) Find an irreducible polynomial of degree 2 over $\mathbb{F}_3$.
   (b) Denote by α a root of this polynomial. Using the basis $1, \alpha$ for $\mathbb{F}_{3^2}$, write down α^2, α^3, and $\alpha^2 + 2\alpha$.
   (c) Let $\xi = 2 + \alpha$ and $\zeta = 2\alpha$. Again using the basis $1, \alpha$ for $\mathbb{F}_{3^2}$, write down $\xi + \zeta$, $\xi\zeta$, ξ^2, and $(2\xi + 1)(\zeta + 2)$.
   (d) Let $\xi = 2 + \alpha$, as above. What is ξ^{-1}, the multiplicative inverse of ξ? (Recall that in a field, every nonzero element must have a multiplicative inverse!)

2. Let K be any field. Show that the map

$$|x| = \begin{cases} 1 & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases} \tag{1}$$

   is an absolute value on K. It is called the *trivial absolute value* on K. What is the trivial valuation on K?

3. Prove property iii) of valuations ($v(x + y) \geq \min(v(x), v(y))$ with equality if $v(x) \neq v(y)$) for general elements $x = \frac{a(T)}{b(T)}$ and $y = \frac{c(T)}{d(T)}$ of $\mathbb{F}_q(T)$.

4. Let $v(x)$ be the valuation on $\mathbb{F}_q(T)$ that was introduced in the lecture (i.e. if $x = \frac{a(T)}{b(T)} \neq 0$, then $v(x) = \deg b(T) - \deg a(T)$, and $v(0) = \infty$). Prove that $|x| = q^{-v(x)}$ is an absolute value.

5. Prove that if an absolute value satisfies the ultrametric inequality ($|x+y| \leq \max(|x|, |y|)$ with equality if $|x| \neq |y|$) then this absolute value is non-Archimedean.

6. Is the trivial absolute value Archimedean or non-Archimedean?

7. For the absolute value $|\cdot|$ on $\mathbb{F}_3(T)$ given in lecture, compute
   (a) $|2T^2 + T|$
   (b) $\left|\dfrac{T^5 + 1}{T^3 + 2T + 2}\right|$
   (c) $\left|\dfrac{T - 1}{T^4 + 2T + 1}\right|$

8. Give 5 "small" elements of $\mathbb{F}_5(T)$, where here by "small" we mean elements with absolute value strictly less than 1. Give 5 "large" elements of $\mathbb{F}_5(T)$, where here by "large" we mean elements with absolute value strictly greater than 1.

9. (adapted from Problem 36 of Gouvêa's *p-adic Numbers, An Introduction*) Consider $|\cdot|$ the absolute value on $\mathbb{F}_q(T)$ given in lecture. This induces, by restriction, an absolute value on $\mathbb{F}_q$. Describe this absolute value.

10. (adapted from Problem 29 of Gouvêa's *p-adic Numbers, An Introduction*) Let A be a domain and K its field of fractions. Let $v\colon A \to \mathbb{R} \cup \{\infty\}$ be a valuation on A. Show that the function $v\colon K \to \mathbb{R} \cup \{\infty\}$ defined by

$$v\left(\frac{a}{b}\right) = v(a) - v(b) \tag{2}$$

for $\frac{a}{b} \in K$ with $a, b \in A$ gives a valuation on K.

11. (adapted from Problem 29 of Gouvêa's *p-adic Numbers, An Introduction*) Let K be a field, v a valuation on K, and e be the usual positive mathematical constant sometimes called Euler's number. Show that the function $|\cdot|\colon K \to \mathbb{R}_+$ given by

$$|x| = e^{-v(x)} \tag{3}$$

for $x \neq 0$ and $|0| = 0$ is a non-Archimedean absolute value on K. Conversely, show that if $|\cdot|$ is non-Archimedean absolute value on K, then $v(\cdot) = -\ln|\cdot|$ is a valuation on K.

12. Prove that in a non-Archimedean field, every triangle is isosceles.

13. Let K be a non-Archimedean field, and recall that for r a positive real number and $a \in K$,

$$B(a, r) = \{x \in K : |x - a| < r\}. \tag{4}$$

(a) Prove that $b \in B(a, r)$ implies that $B(a, r) = B(b, r)$.

(b) Let r and s be two positive real numbers and $a, b \in K$. Prove that

$$B(a, r) \cap B(b, s) \neq \emptyset \tag{5}$$

if and only if

$$B(a, r) \subseteq B(b, s) \quad \text{or} \quad B(b, s) \subseteq B(a, r). \tag{6}$$

(c) (If you know enough topology) Prove that $B(a, r)$ is both open and closed in the topology defined by the metric given by $d(x, y) = |x - y|$.

14. Consider the field $\mathbb{F}_q(T)$ with the absolute value introduced in lecture.

(a) Describe the elements that belong to the ball $B(0,1)$.

(b) Describe the elements that belong to the ball $B(0,q)$.

(c) Describe the elements that belong to the ball $B(0,q^2)$.

(d) Describe the elements that belong to the ball $B(T,1)$.

(e) Describe the elements that belong to the ball $B(T,q)$.

(f) Describe the elements that belong to the ball $B(T^2,1)$.

Lecture 2 :

1. Prove that $\mathbb{F}_q[T]$ is a principal ideal domain.
   Hint: Since there is a division algorithm in $\mathbb{F}_q[T]$, you can use the same proof that is used to show that $\mathbb{Z}$ is a PID, replacing "least element of the ideal" with "element of least degree in the ideal."

2. What are the units in the ring $\mathbb{F}_q[T]$?

3. Let $\widehat{K}$ be a complete field with respect to a non-Archimedean absolute value $|\cdot|$, and for both problems below let $x_n \in \widehat{K}$ for each n.

   (a) Show that the sequence $\{x_n\}_{n=0}^{\infty}$ is Cauchy if and only if $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

   (b) Show that the series $\sum_{n=0}^{\infty} x_n$ converges if and only if $\lim_{n\to\infty} x_n = 0$.

4. Now consider $\widehat{K} = \mathbb{R}$ equipped with the usual absolute value. Then $\mathbb{R}$ is complete with respect to this absolute value, but the absolute value is Archimedean.

   (a) **Updated, this was mistakenly the converse before!**
   Give an example of a sequence $\{x_n\}_{n=0}^{\infty}$ in $\mathbb{R}$ such that $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ but the sequence is not Cauchy.

   (b) Give an example of a series $\sum_{n=0}^{\infty} x_n$ with $x_n \in \mathbb{R}$ such that $\lim_{n\to\infty} x_n = 0$ but the series is not convergent.

5. **Updated: Negative exponent, otherwise it's not Cauchy!**
   Prove that the sequence $\{x_n\}_{n=0}^{\infty}$ for

   $$x_n = \sum_{i=-n}^{0} T^{-i^2} \tag{7}$$

   is Cauchy.

6. (adapted from Goss's *Basic Structures of Function Field Arithmetic*, Chapter 2) Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series with $a_n \in C_\infty$ (where we recall that C_∞ is the completion of the algebraic closure of the completion of $\mathbb{F}_q(T)$ (!)). Define the *order of convergence of* f to be

$$\rho(f) = -\lim_{n\to\infty} \frac{v(a_n)}{n}. \tag{8}$$

Show that if $\alpha \in C_\infty$ then f converges at α if $v(\alpha) > \rho(f)$ and f diverges at α if $v(\alpha) < \rho(f)$.

7. **Updated: This is now a problem.** Let

$$[n] = T^{q^n} - T. \tag{9}$$

Show that $[n]$ is the product of all monic irreducible polynomials of degree dividing n.

8. **Updated: There was a typo in the second formula for D_n before!**
For this problem, let

$$\begin{aligned} D_n &= \prod_{\substack{a\in\mathbb{F}_q[T] \\ a \text{ monic of degree } n}} a \\ &= [n][n-1]^q \cdots [1]^{q^{n-1}}. \end{aligned} \tag{10}$$

   (a) Prove that these two ways to define D_n give the same quantity.

   (b) What is the degree of D_n?

   (c) Let

$$e_C(x) = \sum_{n=0}^{\infty} \frac{x^{q^n}}{D_n}. \tag{11}$$

   What is $\rho(e_C)$, where $\rho(f)$ was defined in equation (8)?

9. For this problem, let

$$\begin{aligned} L_n &= [n][n-1]\cdots[1] \\ &= \text{least common multiple of all monics of degree } n. \end{aligned} \tag{12}$$

   (a) Prove that these two ways to define L_n give the same quantity.

   (b) What is the degree of L_n?

   (c) Let

$$\log_C(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{q^n}}{L_n}. \tag{13}$$

   What is $\rho(\log_C)$, where $\rho(f)$ was defined in equation (8)?

10. Show that $e_C(\log_C(x)) = \log_C(e_C(x)) = x$, where e_C is defined in equation (11) and $\log_C$ is defined in equation (13).

Lecture 3 :

1. Let K be a field of characteristic p and let $\tau_p = x^p$, as in lecture. Prove that the twisted ring $K\{\tau_p\}$ of polynomials in τ_p, where $\tau_p^i = x^{p^i}$, is a non-commutative ring under the usual polynomial addition and composition.

2. Let K be a field and $P(x) \in K[x]$. Prove that P is separable if and only if P and P' are relatively prime. (You may assume that K is algebraically closed if it helps, but it shouldn't be too much more complicated to prove this for general K.)

3. Let K be a field of characteristic p and $P(x) \in K\{\tau_p\}$. Give a simple necessary and sufficient condition for P to be separable.

4. (a) The extension $\mathbb{Q}(\sqrt{-3})$ of $\mathbb{Q}$ is abelian, and therefore contained in $\mathbb{Q}(\zeta_n)$ for some n. What is one such n? (Hint: Actually $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_n)$ for some n, which one?)

   (b) The extension $\mathbb{Q}(\sqrt{5})$ of $\mathbb{Q}$ is abelian, and therefore contained in $\mathbb{Q}(\zeta_n)$ for some n. What is one such n? (Hint: Make a guess based on (a) and check it.) What is the smallest such n?

   (c) The extension $\mathbb{Q}(\sqrt{-7})$ of $\mathbb{Q}$ is abelian, and therefore contained in $\mathbb{Q}(\zeta_n)$ for some n. What is one such n? What is the smallest such n? (Hint: Again, make a guess and check it.)

   (d) For each of the quadratic fields above, what are their discriminants?

   (e) The extension $\mathbb{Q}(\sqrt{-5})$ of $\mathbb{Q}$ is abelian, and therefore contained in $\mathbb{Q}(\zeta_n)$ for some n. What is the smallest such n? (Hint: Depending on how you thought about this problem, this one might break the pattern of parts (a), (b), (c), but part (d) gives you a hint of what you should be thinking about instead.)

We will show next time that

$$e_C(Tz) = Te_C(z) + e_C(z)^q. \tag{14}$$

Accordingly, let's define

$$C_T(z) = T\tau^0 + \tau = Tz + z^q, \tag{15}$$

so that

$$e_C(Tz) = C_T(e_C(z)). \tag{16}$$

More generally, we will see that for each $a \in \mathbb{F}_q[T]$, there is a unique polynomial $C_a(z) \in \mathbb{F}_q[T]\{\tau\}$ such that

$$e_C(az) = C_a(e_C(z)). \tag{17}$$

5. For $a \in \mathbb{F}_q[T]$, let $C_a(z) \in \mathbb{F}_q[T]\{\tau\}$ be as above. Compute the polynomials $C_a(z)$ for
   (a) $a(T) = T^2 + T + 1$
   (b) $a(T) = T + 1$
   (c) $a(T) = T^2 + 3T + 2 = (T + 1)(T + 2)$
   (d) $a(T) = 1$

   Hint: It is possible to do this by only using equation (14) recursively.

6. This question requires the previous question. You can also use that

$$C_{T+2}(z) = (T + 2)\tau^0 + \tau = (T + 2)z + z^q, \tag{18}$$

   and

$$C_{T^2}(z) = T^2\tau^0 + (T^q + T)\tau + \tau^2 = T^2 z + (T^q + T)z^q + z^{q^2}. \tag{19}$$

   (a) From the computation of C_{T^2}, C_{T+1} and C_{T^2+T+1}, guess and prove a formula for $C_{a+b}(z)$ when $a, b \in \mathbb{F}_q[T]$.
   (b) From the computation of C_{T+1}, C_{T+2} and C_{T^2+3T+2}, guess and prove a formula for $C_{ab}(z)$ when $a, b \in \mathbb{F}_q[T]$. (Hint: $C_{ab}(z) \in \mathbb{F}_q[T]\{\tau\}$, what is the multiplication there?)

Lecture 4 :

1. Let $a \in \mathbb{F}_q[T]$. Prove that the a-torsion of the Carlitz module, which is the set

$$\{z \in C_\infty : C_a(z) = 0\}, \tag{20}$$

   is equal to

$$\{e_C\left(\frac{b}{a}\tilde{\pi}\right) : b \in \mathbb{F}_q[T] \text{ and } \deg b < \deg a\}. \tag{21}$$

   Prove that as an $\mathbb{F}_q[T]$-module (where the module structure is given by the Carlitz module), this is isomorphic to $\mathbb{F}_q[T]/(a)$.

2. Construct a Drinfeld module of rank 2 with j-invariant j.

3. Let P be an isogeny $P\colon \phi \to \psi$ of Drinfeld modules over C_∞, by which we mean a function $P\colon C_\infty \to C_\infty$ such that

$$P\phi_a = \psi_a P \tag{22}$$

   for all $a \in \mathbb{F}_q[T]$, and where multiplication here is composition as usual. Prove that $P \in C_\infty\{\tau\}$.

4. Let ϕ be any Drinfeld module over any field. Prove that $\phi_a \phi_b = \phi_b \phi_a$.

5. Compute the ring of endomorphisms of the Drinfeld module of rank 2 given by

$$\phi_T(z) = T\tau^0 + \tau^2, \tag{23}$$

over the field C_∞. (An endomorphism is just an isogeny from a Drinfeld module to itself.)

6. Let ϕ be a Drinfeld module of rank 2 given by

$$\phi_T(z) = T\tau^0 + g\tau + \Delta\tau^2 = Tz + gz^q + \Delta z^{q^2}. \tag{24}$$

Compute $\phi_{2T^2}(z)$.

7. For this problem we will consider a Drinfeld module of rank 2 given by

$$\phi_T(z) = T\tau^0 + g\tau + \Delta\tau^2, \tag{25}$$

with both g and Δ in $\mathbb{F}_q[T]$.

   (a) Compute $\phi_{T+1}(z)$.

   (b) How large is the $(T+1)$-torsion of this Drinfeld module, if we think of it as being defined over C_∞? (It is finite; how many elements does it have?)

   (c) Now think of this Drinfeld modular as being defined over $K = \mathbb{F}_q[T]/(T+1)$. How large is the $(T+1)$-torsion now? (Hint: It depends on whether or not $T+1$ divides g!)