**18.785 Number Theory** **Fall 2021**

**Problem Set #5**

## Description

These problems are related to material in Lectures 9–11. Your solutions should be written in latex and submitted as a pdf-file by midnight on the date due.

Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on, as well any references you consulted that are not listed in the course syllabus. If there are none write "**Sources consulted: none**" at the top of your solution. Note that each student is expected to write their own solutions; it is fine to discuss the problems with others, but your work must be your own.

The first person to spot each typo/error in any of the problem sets or lecture notes will receive 1–5 points of extra credit, depending on the severity of the error

**Instructions:** First do the warm up problems, then solve any combination of problems 1-7 that sum to 96 points and write up your answers in latex. Finally, complete the survey problem 8 (worth 4 points).

## Problem 0.

These are warm up problems that do not need to be turned in.

(a) Prove (1) all local fields have the same cardinality, (2) all global fields have the same cardinality, (3) completing a field with cardinality at least $\#\mathbb{R}$ does not change its cardinality, (4) taking the algebraic closure of an infinite field does not change its cardinality.

(b) Prove that an open subgroup of a topological group is always closed, but a closed subgroup need not be open (give an explicit example).

(c) Prove that $\mathbb{Q}_7(\sqrt[3]{2}) \simeq \mathbb{Q}_7(\zeta_{342})$, where $\zeta_{342}$ is a primitive 342nd root of unity.

(d) Prove that there are exactly two non-isomorphic cubic extensions of $\mathbb{Q}_2$.

## Problem 1. Complete algebraically closed fields (64 points)

The field of complex numbers has the virtue of being both complete and algebraically closed. One might ask whether there are any nonarchimedean fields with this property. We proved in lecture that every finite extension of $\mathbb{Q}_p$ is a local field, and in particular, complete. In this problem you will prove that the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is not complete, but the completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ is both complete and algebraically closed.

**(a)** Prove that if $K$ is a complete perfect field with nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$ then there is a unique absolute value on $\overline{K}$ that restricts to $|\ |$ (so we may unambiguously view $\overline{K}$ as a field with absolute value $|\ |$). You may assume that (all variants of) Hensel's lemma hold for any complete field with a nonarchimedean absolute value (the valuation ring need not be discrete).

**(b)** Let $\overline{\mathbb{Z}}_p := \{x \in \overline{\mathbb{Q}}_p : |x|_p \le 1\}$ be the valuation ring of $\overline{\mathbb{Q}}_p$, with maximal ideal $\mathfrak{m} := \{x \in \overline{\mathbb{Q}}_p : |x|_p < 1\}$. Prove that $\overline{\mathbb{Z}}_p/\mathfrak{m}$ is an infinite algebraic extension of $\mathbb{F}_p$, and that it is algebraically closed (hence we may denote it $\overline{\mathbb{F}}_p$).

**(c)** Prove that the image of $|\ |_p \colon \overline{\mathbb{Q}}_p^\times \to \mathbb{R}_{>0}$ is the set $p^{\mathbb{Q}}$ of fractional powers of $p$. Conclude that $\overline{\mathbb{Z}}_p$ is not a DVR.

**(d)** Prove that $\overline{\mathbb{Z}}_p$ is not compact and $\overline{\mathbb{Q}}_p$ is not locally compact (unlike $\mathbb{Z}_p$ and $\mathbb{Q}_p$).

Recall that a *Baire space* is a topological space in which every countable intersection of open dense sets is dense. The Baire Category Theorem states that every complete metric space (and also every locally compact Hausdorff space) is a Baire space.

**(e)** Let $X_n := \{x \in \overline{\mathbb{Q}}_p : [\mathbb{Q}_p(x) : \mathbb{Q}_p] \leq n\}$. Show that $X_n$ is a closed set whose interior is empty. Conclude that $\overline{\mathbb{Q}}_p$ is not a Baire space and therefore not complete.

**(f)** Prove the following form of KRASNER'S LEMMA: Let $K$ be a complete perfect field with nontrivial nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$, let $\alpha \in \overline{K}$, and let

$$\epsilon := \min\left\{|\alpha - \sigma(\alpha)| : \sigma \in \mathrm{Gal}(\overline{K}/K), \sigma(\alpha) \neq \alpha\right\}.$$

Then $K(\alpha) \subseteq K(\beta)$ for all $\beta \in B_{<\epsilon}(\alpha)$.

**(g)** Prove the following form of CONTINUITY OF ROOTS: Let $K$ be a complete perfect field with nontrivial nonarchimedean absolute value $|\ |$ and algebraic closure $\overline{K}$, and let $\alpha \in \overline{K}$ have minimal polynomial $f(x) = \sum_{i=0}^n f_i x^i \in K[x]$. Prove that for every $\epsilon > 0$ there is a $\delta > 0$ such that if $g(x) = \sum_{i=0}^n g_i x^i \in K[x]$ is a monic polynomial with $\sum_i |g_i - f_i| < \delta$ then $g(x)$ has a root $\beta$ for which $|\alpha - \beta| < \epsilon$.

**(h)** Prove that if $K$ is a complete perfect field with a nontrivial nonarchimedean absolute value then the completion of its algebraic closure is algebraically closed (so in particular, $\mathbb{C}_p$ is algebraically closed).

**Remark**: The simplifying assumption that $K$ is perfect is not necessary; one can prove alternative versions of (f) and (g) that do not assume $K$ is perfect but still imply (h).

## Problem 2. Finite extensions of local fields (64 points)

If $K$ is an archimedean local field, then either $K = \mathbb{R}$, in which case $K$ has exactly one nontrivial finite extension (up to isomorphism), or $K = \mathbb{C}$, in which case $K$ has no nontrivial finite extensions. So let us assume that $K$ is a nonarchimedean local field; then $K$ is a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{F}_p((t))$. For a positive integer $n$, we wish to determine the number of degree-$n$ extensions of $K$ (which we count only up to isomorphism). Let $A$ be the valuation ring of $K$, and let $E_n$ be the set of Eisenstein polynomials $f \in A[x]$ of degree $n$.

First consider the case where $K$ is a finite extension of $\mathbb{Q}_p$:

**(a)** Show that there is a natural topology on $E_n$ induced by the topology on $A$ and that $E_n$ is compact in this topology.

**(b)** Prove that for any finite extension $L/K$, the set

$$\{f \in E_n : K[x]/(f(x)) \simeq L\}$$

is open in the topology on $E_n$.

**(c)** Prove that $K$ has only finitely many totally ramified extensions of degree $n$.

**(d)** Prove that $K$ has only finitely many extensions of degree $n$.

**(e)** Derive a formula for the number of degree-$q$ extensions of $\mathbb{Q}_p$ (up to isomorphism), where $p$ and $q$ are distinct primes.

Now consider the case where $K$ is a finite extension of $\mathbb{F}_p((t))$:

**(f)** Show that $K$ has infinitely many non-isomorphic extensions of degree $n$, for some $n$ (hint: consider extensions $K[x]/(f(x))$ with $f(x) = x^p - x - \alpha$ for some $\alpha \in K$).

**(g)** Why does your proof above for finite extensions of $\mathbb{Q}_p$ not apply here? Pinpoint exactly where the proof breaks down when $\mathbb{Q}_p$ is replaced by $\mathbb{F}_p((t))$.

## Problem 3. Completions of $\mathbb{F}_q(t)$ (32 points)

Recall from Problem 2 of Problem Set 1 that the absolute values $|\ |_\pi$ on $\mathbb{F}_q(t)$ all arise from discrete valuations, all but one of which corresponds to a prime ideal of $\mathbb{F}_q[t]$ that we can uniquely identify by a monic irreducible polynomial $\pi$; let us use $\pi = \infty$ to denote the other discrete valuation $v_\infty(f) := -\deg(f)$, which one can view as the order of vanishing at infinity. Let $\mathbb{F}_q(t)_\pi$ denote the completion of $\mathbb{F}_q(t)$ with respect to the absolute value $|\ |_\pi$, where $q$ is any prime power.

**(a)** Prove that $\mathbb{F}_q(t)_\pi$ is isomorphic to $\mathbb{F}_\pi((T))$, where $\mathbb{F}_\pi$ denotes the residue field of $\mathbb{F}_q(t)$ with respect to $|\ |_\pi$ and $T \in \mathbb{F}_q(t)$ is a uniformizer. For each discrete valuation $\pi$ give an explicit description of the field $\mathbb{F}_\pi$ and the uniformizer $T$ and determine the discrete valuations $\pi$ for which $\mathbb{F}_\pi = \mathbb{F}_q$.

**(b)** Let $\pi_1$ and $\pi_2$ be two discrete valuations for which $\mathbb{F}_{\pi_1} \simeq \mathbb{F}_{\pi_2} \simeq \mathbb{F}_q$ and consider the completions $\mathbb{F}_q(t)_{\pi_1}$ and $\mathbb{F}_q(t)_{\pi_2}$. Are they isomorphic (1) as fields, (2) as $\mathbb{F}_q(t)$-algebras, (3) as topological fields?

**(c)** Now consider the analogous question for completions of $\mathbb{Q}$: for distinct primes $p$ and $q$, are $\mathbb{Q}_p$ and $\mathbb{Q}_q$ isomorphic as (1) fields, (2) $\mathbb{Q}$-algebras, (3) topological fields?

**(d)** Determine the structure of the abelian group $\mathbb{F}_p(t)_\pi^\times/\mathbb{F}_p(t)_\pi^{\times n}$, where $p$ and $n$ are primes and $\pi$ is a discrete valuation on $\mathbb{F}_p(t)$.

Hint for the case $n = p$ in (d): the subgroup $U^{(1)} := 1 + t\mathbb{F}_p[[t]]$ of $\mathbb{F}_p((t))^\times$ is a free $\mathbb{Z}_p$-module of countably infinite rank; each $z = (z_i) \in \mathbb{Z}_p$ acts on $U^{(1)}$ by exponentiation $(1 + tf(t))^z := \lim_{i\to\infty}(1 + tf(t))^{z_i}$ and the set $\{1 + t^m : m \perp p\}$ is a $\mathbb{Z}_p$-basis for $U^{(1)}$.

## Problem 4. The absolute Galois group of $\mathbb{F}_q$ (32 points)

Let $\mathbb{F}_q$ be a finite field with $q$ elements, let $\overline{\mathbb{F}}_q$ be a fixed algebraic closure of $\mathbb{F}_q$, and for every positive integer $n$ let us fix the finite field

$$\mathbb{F}_{q^n} := \{x \in \overline{\mathbb{F}}_q : x^{q^n} = x\}$$

with $q^n$ elements. For any set $S$ (finite or infinite), we use $\#S$ to denote its cardinality (isomorphism class in the category of sets), and if $L/K$ is any field extension, $[L : K]$

denotes the cardinality of any $K$-basis for $L$ (i.e. $\dim_K L$). Recall that cardinals are ordered by monomorphisms of representative sets (so $\#S \leq \#T$ if and only if an injection $f\colon S \to T$ exists), and for any set $S$ we have the strict inequality $2^{\#S} > \#S$ (here $2^{\#S}$ denotes the cardinality of the set of all subsets of $S$). We also note the standard cardinals $\beth_0 := \aleph_0 := \#\mathbb{Z}$, $\beth_1 := 2^{\beth_0} = \#\mathbb{R}$, and $\beth_{n+1} := 2^{\beth_n}$.

**(a)** Prove that $\overline{\mathbb{F}}_q = \bigcup_{n\geq 1} \mathbb{F}_{q^n}$ and compute the cardinals $\#\overline{\mathbb{F}}_q$ and $[\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

Let $\mathbb{N}$ denote the set of positive integers partially ordered by divisibility. Consider the inverse system of groups

$$\big(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathbb{N}},$$

where for $m|n$ the homomorphism $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is induced by restriction (the image of $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is obtained by restricting its domain to $\mathbb{F}_{q^m}$).

**(b)** Prove that we have isomorphisms of abelian groups

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

and that if we view $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$ as an inverse limit of rings we have a ring isomorphism

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p.$$

**(c)** Compute the cardinality of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Conclude that $\#\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \neq [\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

**(d)** Compute the cardinality of the set of subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and the cardinality of the set of subfields $k \subseteq \overline{\mathbb{F}}_q$ that contain $\mathbb{F}_q$. Conclude that the Galois correspondence does not hold for $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$; in particular, many different subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ have the same fixed field $k$ (ridiculously many, in fact).

In later lectures we will see that the Galois correspondence does hold if we regard $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ as a topological group and restrict our attention to closed subgroups.

## Problem 5. Uniqueness of norms (32 points)

Let $K$ be a field with absolute value $|\ |$ and let $V$ be a $K$-vector space. The absolute value $|\ |$ induces a topology on $K$ via the metric $d(x, y) := |x - y|$, and every norm $\|\ \|$ on $V$ induces a topology on $V$ via the metric $d(v, w) := \|v - w\|$.

The goal of this problem is to prove that if $K$ is complete and $V$ has finite dimension then the topology on $V$ is uniquely determined by the topology on $K$. One can find standard proofs for $K = \mathbb{R}$ and $K = \mathbb{C}$ in most analysis textbooks, and the same proof works for any locally compact field. But the standard approach does not work in general because it relies on the assumption that closed balls are compact (as we proved in Lecture 9, this is equivalent to local compactness). Here we follow the approach of Cassels [1], which works for any complete field and any finite-dimensional vector space.

**(a)** Give an example of a complete field that is not locally compact, and give an example of an infinite-dimensional vector space over a complete field with norms that induce different topologies.

Two norms $\| \ \|_1$ and $\| \ \|_2$ on $V$ are said to be *equivalent* if there exists a constant $c \in \mathbb{R}$ such that $\|v\|_1 \leq c\|v\|_2$ and $\|v\|_2 \leq c\|v\|_1$ for all $v \in V$.

**(b)** Show that equivalent norms induce the same topology.

Let us now fix a complete field $K$ and a vector space $V$ with basis $(v_1, \dots, v_n)$, and for $v = x_1v_1 + \cdots x_nv_n \in V$ define the sup-norm $\|v\|_\infty := \max_i |x_i|$.

**(c)** Show that the topology induced by the sup-norm does not depend on the choice of basis and that $V$ is complete in this topology.

**(d)** Let $c := n \max_i \|v_i\|$. Prove that if $\| \ \|$ is a norm on $V$ then $\|v\| \leq c\|v\|_\infty$ for $v \in V$.

**(e)** Prove that if $\| \ \|$ is a norm on $V$ then there is a constant $C \in \mathbb{R}$ such that $\|v\|_\infty \leq C\|v\|$ for $v \in V$ (hint: use induction on $n$). Conclude that every norm on $V$ is equivalent to the sup-norm and thus induces the same topology.

## Problem 6. Cyclotomic number fields (32 points).

Throughout this problem $p$ is a prime, $n$ is a positive integer and $\zeta_n$ denotes a primitive $n$th root of unity. For $p \nmid n$ we define $\mathrm{ord}_n(p)$ as the order of the image of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. In each of the problems below you should prove all equalities included in the statements (they are claims not hypotheses).

**(a)** Prove that for $p \nmid n$ the field $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^r-1})$ is an unramified extension of $\mathbb{Q}_p$ with ring of integers $\mathbb{Z}_p[\zeta_n]$ with $[\mathbb{Q}_p(\zeta_n) : \mathbb{Q}_p] = r = \mathrm{ord}_n(p)$.

**(b)** Prove that $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$ is a totally ramified extension of $\mathbb{Q}_p$ with ring of integers $\mathbb{Z}_p[\zeta_p]$ and degree $p-1$.

**(c)** For all $r \geq 1$ prove that $\mathbb{Q}_p(\zeta_{p^r})$ is a totally ramified extension of $\mathbb{Q}_p$ with ring of integers $\mathbb{Z}_p[\zeta_{p^r}]$ and degree $p^{r-1}(p-1)$.

**(d)** Let $\mathbb{Q}(\alpha)$ be a finite Galois extension of $\mathbb{Q}$, and suppose that for every prime $p$ the ring of integers of $\mathbb{Q}_p(\alpha)$ is $\mathbb{Z}_p[\alpha]$. Show that $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$ and conclude that $\mathbb{Z}[\zeta_n]$ is the ring of integers of $\mathbb{Q}(\zeta_n)$.

**(e)** Derive formulas for the ramification index $e_p$, inertia degree $f_p$, and number of primes $g_p$ of $\mathbb{Q}(\zeta_n)$ above each prime $p$ of $\mathbb{Q}$ as functions of $p$ and $n$.

## Problem 7. Cyclotomic function fields (64 points).

**(a)** Prove that no field of characteristic $p$ contains a primitive $p$th root of unity and that for all positive integers $n$ coprime to $p$ we have $\mathbb{F}_p(t)(\zeta_n) \simeq \mathbb{F}_q(t)$ with $q = p^{\mathrm{ord}_n(p)}$.

It follows from (a) that adjoining a root of unity to a global function field at most changes the field of constants, which is not very interesting. But there are global function fields that play a role very similar to cyclotomic number fields which are often called "cyclotomic function fields", even though they do not involve roots of unity.

The $n$th roots of unity in $\overline{\mathbb{Q}}$ are the elements of $\overline{\mathbb{Q}}^\times$ that lie in the kernel of the "multiplication-by-$n$" endomorphism $[n] \in \mathrm{End}(\overline{\mathbb{Q}}^\times)$. Now $\overline{\mathbb{Q}}^\times$ is a multiplicative group,

so $[n]$ is the map $\alpha \mapsto \alpha^n$ with kernel $\mu_n := \{\alpha \in \overline{\mathbb{Q}} : \alpha^n = 1\}$. The $n$th cyclotomic field is obtained by adjoining the points in $\mu_n$ to $\mathbb{Q}$, which is equivalent to adjoining a primitive $n$th root of unity $\zeta_n$ since $\mu_n = \langle \zeta_n \rangle$ is cyclic. Notice that the map $n \mapsto [n]$ defines a $\mathbb{Z}$-algebra homomorphism $\mathbb{Z} \to \mathrm{End}(\overline{\mathbb{Q}}^\times)$.

We want to replicate this setup in the function field setting, where $\mathbb{Q}$ is replaced by $K := \mathbb{F}_q(t)$ and $\mathbb{Z}$ is replaced by $A := \mathbb{F}_q[t]$. Rather than $n$-torsion points of the multiplicative group $\overline{K}^\times$ we want to instead consider $n$-torsion points of the additive group $\overline{K}^+$. In order to do this we first need to define the "multiplication-by-$n$" maps, by describing the endomorphism $[n] \in \mathrm{End}(\overline{K}^+)$ we associate to each $n \in A$. Note that we have replaced $\mathbb{Z}$ by $A$, so $n$ is not an integer, it is a polynomial in $\mathbb{F}_q[t]$. We first want to understand what elements of $\mathrm{End}(k^+)$ look like when $k$ is an arbitrary field. This is an easy question to answer if we restrict our attention to algebraic endomorphisms defined by a polynomial in $k[x]$.

Let $k$ be a field of characteristic $p \geq 0$. An *additive polynomial* $f \in k[x]$ is a one for which $f(x+y) = f(x) + f(y)$ holds as an identity in $k[x,y]$. Additive polynomials correspond to endomorphisms of $k^+$ and include the maps $x \mapsto ax$ defined by linear monomials, and in positive characteristic, the Frobenius map $x \mapsto x^p$.

In fact these two examples generate all additive polynomials.

**(b)** Prove that $f \in k[x]$ is an additive polynomial if and only if $f(x) = \sum_{i=0}^{r} a_i x^{p^i}$ for some $a_i \in k$, with $r = 0$ if $p = 0$.

Now assume $p > 0$, and let $\mathcal{A}(k) \subseteq \mathrm{End}(k^+)$ denote the set of additive polynomials in $k[x]$, viewed as endomorphisms of $k^+$. They form a non-commutative ring under addition and composition.

**(c)** Let $k\{\tau\}$ denote the *twisted polynomial ring* in $\tau$, in which $\tau a = a^p \tau$ for all $a \in k$. Show the map $\tau \mapsto x^p$ and $a \mapsto ax$ for $a \in k$ is a ring isomorphism $k\{\tau\} \to \mathcal{A}(k)$.

We now return to our function field setting with $K = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$. Let $L$ be a (not necessarily finite) extension of $K$, and let $\mathcal{A}(L)$ denote the set of additive polynomials that are also $\mathbb{F}_q$-linear (for $q = p$ this is all additive polynomials, but for $q \neq p$ it is the subring generated by linear monomials and the $q$-power Frobenius).

A *Drinfeld $A$-module over $L$* is defined by an $\mathbb{F}_q$-algebra homomorphism

$$\begin{aligned} A &\to \mathcal{A}(L) \\ a &\mapsto [a] \end{aligned}$$

such that $[a] \in \mathcal{A}(L) \subseteq L[x]$ has linear coefficient $a$ but not every $[a] \in \mathcal{A}(L)$ is linear. The map $a \mapsto [a]$ allows us to to view $L^+$ as an $A$-module with multiplication defined by $a \cdot \alpha := [a](\alpha)$; note that this is not the usual multiplication $a\alpha$ in $L$ (which gives a different $A$-module structure), we are evaluating the polynomial $[a] \in L[x]$ at $\alpha \in L$.

To specify a Drinfeld $A$-module it is enough to specify $[t]$, the image of $t \in A = \mathbb{F}_q[t]$ in $\mathcal{A}(L) \subseteq L[x]$, since this uniquely determines an $\mathbb{F}_q$-algebra homomorphism. The *rank* of a Drinfeld $A$-module is the positive integer $\log_q \deg[t]$ (the degree of an $\mathbb{F}_q$-linear additive polynomial is a power of $q$).

The simplest example of a $A$-Drinfeld module is the *Carlitz module*, with $L = \overline{K}$ and $A \mapsto \mathcal{A}(L)$ defined by $[t] := x^q + tx$, which is a Drinfeld module of rank 1. This

is the only Drinfeld $A$-module we shall consider, and henceforth for any $n \in A$ we use $[n]$ to denote the image of $n$ under the $\mathbb{F}_q$-algebra homomorphism defined by the Carlitz module. For example, we have

$$[t^2] = [t]^2 = (x^q + tx)^q + t(x^q + tx) = x^{q^2} + (t^q + t)x^q + t^2x.$$

To simplify matters, we will henceforth work with $K = \mathbb{F}_p(t)$ and $A = \mathbb{F}_p[t]$.

**(d)** Let $\pi \in A = \mathbb{F}_p[t]$ be monic irreducible. Prove $[\pi - 1](a) \equiv 0 \bmod \pi$ for all $a \in A$ (hint: prove $[\pi] \equiv x^{p^{\deg \pi}} \bmod \pi$ by showing that if its reduction has any nonzero roots it must have $p^{\deg \pi}$ distinct roots, and that this is impossible).

For monic $n \in A$ we define the *Carlitz $n$-torsion module* $\Lambda_n := \{\alpha \in \overline{K} : [n](\alpha) = 0\}$, and we view $K(\Lambda_n)$ as the "$n$th cyclotomic field" of $K$. As you may wish to verify, $\Lambda_n$ is a submodule of the Carlitz module (this means $[a](\alpha) \in \Lambda_n$ for all $a \in A$ and $\alpha \in \Lambda_n$). The restriction to monic $n$ corresponds to the restriction to positive $n \in \mathbb{Z}$ when considering $n$th roots of unity, it distinguishes a generator for $nA$ and ensures $nA \neq \{0\}$.

**(e)** For $K = \mathbb{F}_p(t)$ prove $K(\Lambda_t) \simeq K((-t)^{1/(p-1)})$ (compare to part (b) of Problem 6).

**(f)** For $a, b \in A$ prove that $a \equiv b \bmod n$ if and only if $[a](\alpha) = [b](\alpha)$ for $\alpha \in \Lambda_n$.

**(g)** Show that $\Lambda_n$ is a cyclic $(A/nA)$-module generated by any $\lambda_n \in \Lambda_n$ that does not lie in $\Lambda_m$ for any $m$ properly dividing $n$, and that $\{[a](\lambda_n) : a \in A \text{ with } a \perp n\}$ is the set of all generators. Then show that the map $a \mapsto [a](\lambda_n)$ defines an $A$-module isomorphism $A/nA \simeq \Lambda_n$, where the $A$-module structure on $A/nA$ is the usual one given by multiplication by elements of $A$ reduced module $nA$.

**(h)** For each of $n = t^2 + 1, t^2 + t + 1, t^2 - t + 1 \in A = \mathbb{F}_3[t]$ give a list of representatives for $A/nA$ indicating which correspond to generators of $\Lambda_n$ under the isomorphism defined in (g) and describe the structure of the abelian group $(A/nA)^\times$.

**(i)** Let $n \in A$ be nonzero. Prove that for each $\sigma \in \mathrm{Gal}(K(\Lambda_n)/K)$ there is a unique $a_\sigma \in (A/nA)^\times$ for which $\sigma(\alpha) = [a_\sigma](\alpha)$ for all $\alpha \in \Lambda_n$. Then show the map $\sigma \mapsto a_\sigma$ defines a group isomorphism $\mathrm{Gal}(K(\Lambda_n)/K) \xrightarrow{\sim} (A/nA)^\times$.

It follows from (i) that for each monic $n \in A$ we have an abelian extension $K(\Lambda_n)/K$ with Galois group $(A/nA)^\times$, just as for every $n \in \mathbb{Z}_{>0}$ we have an abelian extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$, and in fact more is true. The Kronecker-Weber theorem which we will prove in later lectures states that every abelian extension of $\mathbb{Q}$ is a subfield of some $\mathbb{Q}(\mu_n)$, and the Carlitz-Hayes theorem states that every abelian extension of $K = \mathbb{F}_q(t)$ is a subfield of some $K(\Lambda_n)$. This is the motivation for referring to the fields $K(\Lambda_n)$ as cyclotomic function fields.

## Problem 8. Survey (4 points)

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

| | Interest | Difficulty | Time Spent |
|---|---|---|---|
| Problem 1 | | | |
| Problem 2 | | | |
| Problem 3 | | | |
| Problem 4 | | | |
| Problem 5 | | | |
| Problem 6 | | | |
| Problem 7 | | | |

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

| Date | Lecture Topic | Material | Presentation | Pace | Novelty |
|---|---|---|---|---|---|
| 10/11 | Extensions of complete DVRs | | | | |
| 10/18 | Totally ramified extensions | | | | |
| 10/20 | The different and discriminant | | | | |

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

## References


[1] J.W.S. Cassels, *Local fields*, Cambridge University Press, 1986.

[2] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta functions*, Springer, 1984.

18.785 Number Theory I
Fall 2021