**18.785 Number Theory** **Fall 2025**
**Problem Set #3** **Due: 09/26/2025**

---

These problems are related to material in Lectures 4–6. Your solutions should be written up in latex and submitted as a pdf-file to Gradescope by midnight on the date due.

**Instructions:** Solve Problem 0, then pick any combination of problems that sum to 100 points. Collaboration is permitted/encouraged, but you must identify your collaborators (including any LLMs you consulted) and any references you consulted outside the course syllabus. Include this information after the **Collaborators/Sources** prompt at the end of the problem set (if there are none, you should enter "none", do not leave it blank). Each student is expected to write their own solutions; it is fine to discuss problems with others, but your writing must be your own.

## Problem 0. Warmup (0 points)

These warmup exercises do not need to be written up.

**(a)** Let $K$ be the field $\mathbb{F}_p(x,y)$ and consider the field $L := K[t]/(t^{p^2} + t^p x + y)$. Show that $L/K$ can be decomposed as a purely inseparable extension of a separable extension, but not as a separable extension of a purely inseparable extension.

**(b)** Show that the étale algebra $\mathbb{F}_2^3$ is not isomorphic to $\mathbb{F}_2[x]/(f)$ for any $f \in \mathbb{F}_2[x]$.

**(c)** Let $K$ and $L$ be two number fields. Describe the finite ètale $K$-algebra $L \otimes_{\mathbb{Q}} K$ when $L \subseteq K$, $K \subseteq L$, $K = L$, $K \cap L = \mathbb{Q}$, and then in general.

## Problem 1. Perfect closures (33 points)

Let $k$ be a field. A purely inseparable algebraic extension of $k$ that is perfect is called a *perfect closure* of $k$.

**(a)** Prove that every field has a perfect closure.

**(b)** Prove that the perfect closure is unique up to a unique isomorphism: if $L_1$ and $L_2$ are two perfect closures of $k$ then there is a unique $k$-algebra isomorphism $L_1 \to L_2$.

In view of **(b)**, we use $k^{\text{perf}}$ to denote the (essentially unique) perfect closure of $k$.

**(c)** Let $L$ be a separable extension of $k$ and let $M$ be a purely inseparable extension of $k$. Show that the $k$-algebra $L \otimes_k M$ is a field (Hint: Reduce to finite extensions and show that the quotient of $L \otimes_k M$ by a maximal ideal has the same degree).

**(d)** Let $\bar{k}$ be an algebraic closure of $k$, let $k^{\text{sep}}$ be the separable closure of $k$ in $\bar{k}$, and let $k^{\text{perf}}$ be the perfect closure of $k$ in $\bar{k}$. Let $L$ be the $k$-algebra $k^{\text{sep}} \otimes_k k^{\text{perf}}$, which by **(c)** is a field. Show that $L$ is an algebraic extension of both $k^{\text{sep}}$ and $k^{\text{perf}}$ and can thus be embedded in $\bar{k}$. Then show that this embedding is an isomorphism.

## Problem 2. Counting irreducible polynomials over finite fields (33 points)

Let $k$ be a finite field. Let $q = \#k$. For $d \geq 1$, let $N_d$ be the number of degree $d$ monic irreducible polynomials in $k[x]$.

**(a)** Adapt the proof of the Euler product identity

$$\sum_{n \geq 1} n^{-s} = \prod_{\text{prime } p} (1 + p^{-s} + p^{-2s} + \cdots)$$

to prove the function field analogue

$$\sum_{\text{monic } f \in k[x]} x^{\deg f} = \prod_{\text{monic irreducible } g \in k[x]} (1 + x^{\deg g} + x^{2 \deg g} + \cdots).$$

**(b)** Prove $(1 - qx)^{-1} = \prod_{d \geq 1} (1 - x^d)^{-N_d}$ in $\mathbb{Z}[[x]]$.

**(c)** Prove $q^n = \sum_{d|n} d N_d$ for each $n \geq 1$.

**(d)** Prove $N_n = \frac{1}{n} \sum_{d|n} \mu(n/d)\, q^d$ for each $n \geq 1$.

**(e)** Prove that for every $n \geq 1$, there exists a degree $n$ monic irreducible $f \in k[x]$.

**(f)** Prove that a random monic $f \in k[x]$ of degree $n$ is irreducible with probability $\frac{1}{n} + O(n^{-1} q^{-n/2})$.

**(g)** Use the theory of finite fields to give an alternative proof of the formula in **(c)** by grouping elements of $\mathbb{F}_{q^n}$ by minimal polynomial.

## Problem 3. Class groups of quadratic rings (33 points)

Let $A = \mathbb{Z}[\sqrt{-5}]$.

**(a)** Prove that each ideal class in $A$ is represented by a fractional ideal $I$ in which 1 is an element of smallest complex absolute value.

**(b)** Prove that the only such fractional ideals are $(1)$ and $(1, (1 + \sqrt{-5})/2)$.

**(c)** Compute the ideal class group $\mathrm{cl}(A)$.

Now let $A = \mathbb{Z}[\sqrt{-d}]$ for some positive integer $d$.

**(d)** Prove that there is a constant $B$ depending on $d$, such that any set of more than $B$ points in the rectangle $R := [0,1] + [0, \sqrt{d}]i$ contains two distinct points separated by a distance less than 1.

**(e)** Prove that if $I$ is a fractional ideal in which 1 is an element of smallest complex absolute value, then $[I : A] \leq B$.

**(f)** Prove that for each $n \geq 1$, there are only finitely many fractional ideals $I$ with $A \subseteq I \subseteq \operatorname{Frac} A$ and $[I : A] = n$.

**(g)** Prove that $\mathrm{cl}(A)$ is finite.

## Problem 4. Factoring primes in quadratic fields (33 points)

Let $p, q \in \mathbb{Z}$ denote (not necessarily distinct) primes.

**(a)** Let $K$ be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$ As we proved in Lecture 5, $\mathcal{O}_K$ is a Dedekind domain (as are all rings of integers). Let

$$(q) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

be the unique factorization of the principal ideal $(q)$ in $\mathcal{O}_K$. Show that

$$[\mathcal{O}_K : q\mathcal{O}_K] = q^2 = \prod_{i=1}^{n} [\mathcal{O}_K : \mathfrak{q}_i]^{e_i},$$

(where $[B : A]$ denotes the index of $A$ in $B$ as an additive abelian group), and conclude that there are three possibilities: $(q)$ is prime, $(q) = \mathfrak{q}_1\mathfrak{q}_2$, or $(q) = \mathfrak{q}_1^2$.

**(b)** For $K := \mathbb{Q}(\sqrt{p})$ determine the unique factorization of $(q)$ in $\mathcal{O}_K$ explicitly; that is, determine which of the three possibilities admitted by **(a)** occurs and when applicable, write $\mathfrak{q}_i$ in the form $(q, \alpha_i)$ for some explicitly described $\alpha \in \mathcal{O}_K$. Be sure to address the cases $q = 2$ and $q = p$ which may require special treatment.

**(c)** Do the same for $K := \mathbb{Q}(\sqrt{-p})$.

**(d)** For primes $p, q \neq 2$, let $K := \mathbb{Q}(\sqrt{\pm p})$ and relate the factorization of $(q)$ in $\mathcal{O}_K$ you determined in parts (b) and (c) to the factorization of $x^2 \mp p$ in $\mathbb{F}_q[x]$.

## Problem 5. Computing norms and traces (33 points)

Let $L/K$ be a finite extension of fields, let $\overline{K}$ be an algebraic closure containing $L$, and let $\Sigma := \mathrm{Hom}_K(L, \overline{K})$. Let $\alpha \in L$ have minimal polynomial $f(x) = \sum_{i=0}^{d} a_i x^i \in K[x]$, and let $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ its factorization in $\overline{K}[x]$. Define $n := [L : K]$ and $e := [L : K(\alpha)]$.

**(a)** Prove that

$$\mathrm{N}_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{d} \alpha_i = (-1)^d a_0 \qquad \text{and} \qquad \mathrm{T}_{K(\alpha)/K}(\alpha) = \sum_{i=1}^{d} \alpha_i = -a_{d-1}.$$

(Hint: Consider the companion matrix of $f$).

**(b)** Show that if $L/K$ is purely insepararable then

$$N_{L/K}(\alpha) = \alpha^{[L:K]} \qquad \text{and} \qquad T_{L/K}(\alpha) = [L : K]\alpha = \begin{cases} \alpha & \text{if } L = K \\ 0 & \text{if } L \neq K \end{cases}.$$

**(c)** Prove that

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{d} \alpha_i^e = (-1)^n a_0^e \qquad \text{and} \qquad \mathrm{T}_{L/K}(\alpha) = \sum_{i=1}^{d} e\alpha_i = -ea_{d-1}.$$

**(d)** Prove that for all $\alpha \in L$ we have

$$N_{L/K}(\alpha) = \left(\prod_{\sigma\in\Sigma} \sigma(\alpha)\right)^{[L:K]_i} \qquad \text{and} \qquad T_{L/K}(\alpha) = [L:K]_i \left(\sum_{\sigma\in\Sigma} \sigma(\alpha)\right).$$

**(e)** Prove that $T_{L/K} = 0$ (as a linear map) if and only if $L/K$ is inseparable. (Hint: Use base change to handle the separable case.)

## Problem 6. Survey (1 point)

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 | | | |

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

**Collaborators/sources**: