PAWS 2024: LOCAL FIELDS
PROBLEM SET 0

JACKSYN BAKEBERG, THOMAS BROWNING, ANNA DIETRICH, SIDNEY WASHBURN

Welcome to PAWS! Below are the exercises for Problem Set 0, which are intended to provide some background on common vocabulary and notation that will be used in this course. The exercises are organized into review problems and advanced problems. You are absolutely not obligated (or expected) to finish all of these problems before our first meeting, but we recommend that you at least attempt the problems in the review section if you have not seen the material before. Most importantly, work on the problems that interest you!

Review Problems

Problem 1. Let $x_1, x_2, \ldots$ be elements of $\mathbb{R}$. We call (x_n) a *sequence* and say that the sequence (x_n) *converges* to a real number L if for every $\varepsilon > 0$, there exists an integer N such that $|x_n - L| < \varepsilon$ for all $n \geq N$.

(1) Suppose that a sequence (x_n) converges to x and also converges to y. Show that $x = y$.
(2) Suppose that a sequence (x_n) converges to x and a sequence (y_n) converges to y. Show that the sequence $(x_n + y_n)$ converges to $x + y$. Show that $(x_n y_n)$ converges to xy as well.

Problem 2. A subset $S \subseteq \mathbb{R}$ is said to be *open* if for all $x \in S$, there exists an "open ball"

$$B(x, r) = \{y \in \mathbb{R} : |x - y| < \varepsilon\}$$

contained in S. A subset S is said to be closed if its complement S^c is open.

(1) Let $a < b$ be real numbers. Show that the interval (a, b) is open but not closed, that $[a, b]$ is closed but not open, and that $[a, b)$ and $(a, b]$ are neither open nor closed.
(2) Show that an arbitrary union of open sets is open. Give an example where an arbitrary intersection of open sets is not open.
(3) Show that a subset U is closed if and only if the limit points of all convergent sequences in U are contained in U.

Problem 3. The field $\mathbb{Q}(i)$ consists of all complex numbers $a + bi$ with $a, b \in \mathbb{Q}$.

(1) Compute $(1 + i)^{-1}$.
(2) Show that for any nonzero element $a + bi \in \mathbb{Q}(i)$, the inverse $(a + bi)^{-1}$ indeed lies in $\mathbb{Q}(i)$.

Problem 4. One definition of characteristic can be stated with the notion of *additive order*. If F is a field, and $a \in F$, then the additive order of a is the smallest integer n such that na is equal to 0. The *characteristic* of a field $\mathrm{char}(F)$ is 0 if the additive order of every nonzero element of F is infinite, and is $0 < p < \infty$ if the additive order of every nonzero element is p. If $\mathrm{char}(F) = p > 0$, then F has *finite characteristic*.

(1) Show that if $\mathrm{char}(F) = p > 0$, then p must be prime.
(2) Show that $\mathbb{Z}/p\mathbb{Z}$ (the integers modulo p, also called $\mathbb{F}_p$) is a field of characteristic p.
(3) Show that if $\mathrm{char}(F) = p > 0$, then $\mathbb{F}_p$ embeds into F.
(4) Show that if F is a finite field containing a subfield K with p elements, then F has p^m elements, with $m = [F : K]$ (the degree of F as a vector space over K).
(5) Give an example of an infinite field with finite characteristic.

Problem 5. In a domain R (a ring with no zero-divisors), an element $x \in R$ is *prime* if $x \mid ab$ implies $x \mid a$ or $x \mid b$, for any $a, b \in R$. An element $x \in R$ is *irreducible* if x cannot be expressed as the product of two non-units in R.

(1) Prove that if $x \in R$ is prime, then x is irreducible.

A domain R is a *unique factorization domain* (abbreviated UFD) if every non-zero element $x \in R$ can be expressed as a product $x = u \cdot p_1^{e_1} \cdots p_r^{e_r}$, where u is a unit and each p_i is irreducible, and the p_i are unique up to permutation and rescaling by a unit.

(2) The ring $R = \mathbb{Z}[i]$ happens to be a UFD. Factor 2, 3, and 5 in R.

Hint: Any factorization must be into elements of smaller absolute value.

Although there are domains that are not UFDs, this lecture series will only focus on rings that are UFDs. And in a UFD, irreducible elements are prime, so we won't have to worry about the distinction between primes and irreducibles.

Problem 6. A domain R is a *principal ideal domain* (abbreviated PID) if every ideal of R is principal. All PIDs are also UFDs. The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{F}_q[t]$ are all examples of PIDs and are thus UFDs.

Prove that if R is a PID, then a principal ideal (x) is maximal if and only if x is irreducible.

Problem 7. Given a domain R, the *fraction field* of R is the set of symbols of the form a/b, where $a, b \in R$, $b \neq 0$. Two fractions a/b and c/d are declared equal if $ad = bc$. Formally, if F denotes the fraction field, then $F = (R \times (R - \{0\}))/\sim$, where $(a, b) \sim (c, d) \iff ad = bc$.

(1) We can equip F with an addition and multiplication law as follows: $a/b + c/d := (ad + bc)/bd$ and $(a/b) \cdot (c/d) := (ab)/(cd)$. Prove that the addition and multiplication laws are well-defined. (e.g. show that if $a/b \sim a'/b'$ and $c/d \sim c'/d'$, then $a/b + c/d \sim a'/b' + c'/d'$.)
(2) Prove that F is a ring.
(3) Prove that F is a field.
(4) What is the field of fractions of $\mathbb{Z}$? $\mathbb{Z}[i]$? $\mathbb{Q}[t]$?
(5) Prove that if R is already a field, then R is isomorphic to its fraction field.

Problem 8. Suppose that R is a ring. A *left R-module* M is an abelian group M and a map $R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, the following properties hold:

(a) $r(x + y) = rx + ry$,
(b) $(r + s)x = rx + sx$,
(c) $(rs)x = r(sx)$, and
(d) $1(x) = x$.

A right R-module can be defined similarly with a map $M \times R \to M$. Note that if R is commutative, then right and left modules are the same. For this problem, you may assume that all rings are commutative.

(1) Let M be an R-module. Show that for all $m \in M$, $0(m) = 0$, and $-1(m) = -m$.
(2) Show that R is a module over itself.
(3) Let I be an ideal of R. Show that I and R/I are R-modules.
(4) What is another name for a module over a field?

A module M is called *finitely generated* over R if it has a finite basis $m_1, \ldots, m_k$.

(5) Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.
(6) Explain why being a $\mathbb{Z}$-module means the same thing as being an Abelian group.

Problem 9. We can also define characteristic categorically. An object A in a category $\mathcal{C}$ is called *initial* if there is a unique morphism $A \to B$ for all objects B in $\mathcal{C}$.

(1) Show that $\mathbb{Z}$ is an initial object in the category of rings. In other words, show that for every ring R, there is a unique ring homomorphism $\mathbb{Z} \to R$.

From part (1), there is a unique homomorphism $\tau : \mathbb{Z} \to F$ for all fields F. The characteristic of a field F is then defined to be the non-negative generator of the ideal $\ker \tau$.

(2) Show that if $\operatorname{char}(F) = 0$, then $\mathbb{Q}$ embeds into F.
(3) Show that if $k \subset K$ is a field extension, then $\operatorname{char}(k) = \operatorname{char}(K)$.

(4) Use the categorical definition of characteristic to show that $\mathrm{char}(F)$ is either 0 or prime.

Advanced Problems

Problem 10. Prove the sum $\sum_p 1/p$ diverges in the steps below. Note that this proof *does not* assume there are infinitely primes in $\mathbb{Z}$. Make sure to justify any operations you perform on infinite sums/products.

(1) Let $p_1, p_2, ..., p_{\ell(n)}$ be the primes less than n and put $\lambda(n) = \prod_{i=1}^{\ell(n)} \frac{1}{(1-1/p_i)}$. Prove

$$\lambda(n) = \sum_{a_1,\ldots,a_\ell \geq 0} \frac{1}{p_1^{a_1} \cdots p_\ell^{a_\ell}}.$$

(2) Prove $\lambda(n) \to \infty$ as $n \to \infty$.

(3) Calculate that

$$\log \lambda(n) = \left(\sum_{i=1}^{\ell} 1/p_i\right) + \sum_{i=1}^{\ell} \sum_{m \geq 2} 1/(mp_i^m).$$

(4) Prove

$$\log \lambda(n) < \left(\sum_{i=1}^{\ell} 1/p_i\right) + 2\sum_{i=1}^{\ell} p_i^{-2},$$

and conclude $\sum_p 1/p$ diverges.

(5) Adapt the proof above to prove that $\sum_f 1/p^{\deg(f)}$ diverges, where the sum runs over monic irreducible polynomials in $\mathbb{F}_q[t]$.

Problem 11.

(1) Let $X \subseteq \mathbb{R}$. Suppose that for every decreasing sequence of nonempty closed subsets

$$X \supset K_1 \supset K_2 \supset K_3 \supset \cdots,$$

the intersection $\bigcap_{n=1}^{\infty} K_n$ is nonempty. Show that every sequence (x_n) in X has a convergent subsequence.

(2) Is the converse true? Prove or disprove.

Problem 12. Throughout this problem, you may use the fact that $\mathbb{F}_p^\times$ is cyclic (isomorphic to the additive group $\mathbb{Z}/(p-1)\mathbb{Z}$).

(1) Fix an odd prime p. For $a \in \mathbb{F}_p^\times$, define $(a/p) := 1$ if a is a square in $\mathbb{F}_p$ and $(a/p) := -1$ otherwise. Prove that $(\cdot/p) : \mathbb{F}_p^\times \to \{\pm 1\}$ is surjective homomorphism.

(2) Prove that there is only one surjective homomorphism $\mathbb{F}_p^\times \to \{\pm 1\}$.

(3) Prove $(a/p) \equiv a^{(p-1)/2} \bmod p$.

(4) Prove that an odd prime p can be expressed as a sum of two integer squares iff $p \equiv 1$ modulo 4. (Hint: Consider p as an element of $\mathbb{Z}[i]$ and the quotient $\mathbb{Z}[i]/(p)$).