READING SEMINAR: PRIMES OF THE FORM $x^2 + ny^2$

Starters

(1) Ring of integers
   (a) Define number fields, ring of integers, Dedekind domains.
   (b) Explain the unique factorization of ideals.
   (c) Define fraction ideals and ideal class group.
   (d) Explain (b),(c) in the case of algebraic curves.

(2) Ramification
   (a) Define ramification index, inertial degree.
   (b) Draw a table, compare the notions: unramified, totally split, tamely ramified, totally ramified.
   (c) Determine the ramification behavior of prime in a monic extension.
   (d) Work out everything for quadratic extension.

(3) The Frobenius
   (a) Define the decomposition group and inertia group.
   (b) Explain the sequence:

$$0 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathrm{P})/\kappa(\mathfrak{p})) \to 0.$$

   (c) Define the Frobenius element.
   (d) Introduce the Legendre symbol and quadratic reciprocity.

Entrees

(1) Hilbert class field
   (a) Define the Artin symbol.
   (b) Justify the notion of maximal unramified extension.
   (c) Define the Hilbert class field.
   (d) Artin Reciprocity theorem+Galois theory$\Rightarrow$ Class field theory.

(2) Proof of main result, when $n \neq 1 (\mathrm{mod}\ 4)$, n square free.
   (a) Explain: $p = x^2 + ny^2$ iff p totally splits in $\mathrm{Hilb}(\mathbb{Q}(\sqrt{-n}))$.
   (b) Carefully explain the proof.
   (c) Show $\mathrm{Hilb}(\mathbb{Q}(\sqrt{-14})) = \mathbb{Q}(\sqrt{\sqrt{2}-1}, \sqrt{-14})$.
   (d) Other examples, $\mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{-10}), \mathbb{Q}(\sqrt{-35})$ and $\mathbb{Q}(\sqrt{-17}), \mathbb{Q}(\sqrt{-55})$.

Specials

(1) Historical remark: Genus theory
   (a) Explain terminologies, uniqueness of reduced primitive positive definite forms.
   (b) Genus of quadratic forms with a fixed discriminant.
   (c) Use genus theory to prove some old results.
   (d) Explain why the genus theory cannot deal with $n = 14$.

(2) Class field theory
   (a) Artin reciprocity theorem in terms of modulus.
   (b) Explain the conductor theorem.
   (c) Explain The existence theorem.
   (d) Prove the Kronecker-Weber theorem.

(3) Chebotarev's theorem
   (a) Explain the theorem.
   (b) Show there are infinitely primes in arithemtic progression.
   (c) Show there are infinitely many prime represented by a primitive quadratic form.
   (d) Show splitting behaviour of primes determine the extension.

(4) Complex multiplication and class field.
   (a) Define elliptic curves.
   (b) Weierstrass functions and equation.
   (c) Define j-invariant.
   (d) Show the class field is generated by the $j(\mathbb{C}/\mathfrak{a})$.

Sides

(1) Ring class field,
   (a) $p = x^2 + ny^2$ for all n.
   (b) Norm primes, primes of the form $p = x^3 + 11b^3 + 121c^3 - 33abc$

(2) Orders in imaginary quadratic fields
   (a) Define orders.
   (b) Define class group of orders.
   (c) Explain $\mathrm{Cl}(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I(\mathcal{O}_K, f)/P(\mathcal{O}_K, f)$.
   (d) Explain the notions in the case of algebraic curves.

(3) The two class groups
   (a) Define form class group.
   (b) Prove form class group coincide with ideal class group.