Math 620 (Algebraic Number Theory I), PS 6 (three pages)

(Bi)quadratic number fields  Let $d, d', d'' \in \mathbb{Z}$ be square free.

1) Let $K = \mathbb{Q} [\sqrt{d}]$, $d < 0$, and $N : K \rightarrow \mathbb{Q}$ the norm. Prove/disprove/answer:
   a) $\mathcal{O}_K$ is Euclidean w.r.t. the norm iff $d = -1, -2, -3, -7, -11$.
   b) Find all the prime numbers of the form $p = x^2 + y^2 = x_2^2 + 2y_2^2 = x_3^2 + x_3y_3 + y_3^2$ with $x_i, y_i \in \mathbb{Z}$. How many such representations are there for a given $p$?
   - Same question for natural numbers $n$.
   c) Describe the units $U_K$ of $K$. What is the maximal cardinality of $U_K$?

2) Let $K = \mathbb{Q} [\sqrt{d}]$ be an arbitrary quadratic number field. Prove/disprove/answer:
   a) Verify the ramification criterion directly.
   b) Suppose that $d > 0$, and fix an embedding $i : K \hookrightarrow \mathbb{R}$. (How many such embeddings are there?) There is a unique unit $\varepsilon \in U_K$ s.t. $i(\varepsilon) > 1$ is minimal with this property.
   - If so, then $U_K = \{ \pm 1 \} \cdot \varepsilon^2$.
   c) Find the unit $\varepsilon$ in the case $d = 2, 3, 5, 6, 7, ...$ Could you solve this problem in general?
   d) Find prime numbers which are the form $p = x^2 + y^2 = x_2^2 + 2y_2^2 = x_3^2 + x_3y_3 + y_3^2$ with $x_i, y_i \in \mathbb{Z}$. How many such representations are there for a given $p$?
   - Same question for natural numbers $n$.
   [Hint to b): Let $K$ by any number field. For every real numbers $\varepsilon' < \varepsilon''$ there exist only finitely many elements $a \in \mathcal{O}_K$ such that $\varepsilon' \leq |a(\varepsilon)| \leq \varepsilon''$ for all embeddings $i : K \rightarrow \mathbb{C}$ [why?], etc.]

3) Let $K' = \mathbb{Q} [\sqrt{d}]$ and $K'' = \mathbb{Q} [\sqrt{d''}]$ be two quadratic number fields. Their compositum $K = K'K''$ is called a biquadratic number field. Prove/disprove/answer:
   a) There exist $d'_0, d''_0 \in \mathbb{Z}$ relatively prime such that $K = \mathbb{Q} [\sqrt{d'_0}, \sqrt{d''_0}]$.
   b) Suppose that $(d', d'') = 1$. Then $\mathcal{O}_K = \mathcal{O}_{K'} \mathcal{O}_{K''}$ iff $d'd''(d'_0 - 1)(d''_0 - 1) \equiv 0 \pmod{8}$.
   c) Give a basis of $\mathcal{O}_K$ in general, and analyze the behavior of prime numbers in $\mathcal{O}_K$.

Cubic number fields  $K = \mathbb{Q} [\alpha]$ with $\alpha^3 = d \in \mathbb{Q}$ is called a cubic number field.

4) Show that each cubic field is of the form $K = \mathbb{Q} [\alpha]$ with $\alpha^3 = d$, where form $d = d_1d_2^2$ with $d_1, d_2 \in \mathbb{Z}$ positive square free relatively prime integers.

5) Let $K = \mathbb{Q} [\alpha]$ be a cubic field.
   a) In the case $\alpha^3 = 5$, find $\mathcal{O}_K$ and give a description of the decomposition of prime numbers in $\mathcal{O}_K$.
   b) Prove or disprove: 3 is always ramified in a cubic number field. Prove directly that $|\delta_K| > 1$ for $K$ a cubic number field.
   c) Try to give a comprehensive description of $\mathcal{O}_K$ starting from $d = d_1d_2^2$.

Hilbert Decomposition Theory

6) Describe the decomposition/inertia/ramification groups of primes in quadratic number fields $K = \mathbb{Q} [\sqrt{d}]$. The same question for bi-quadratic number fields $K = \mathbb{Q} [\sqrt{d'}, \sqrt{d''}]$. 

1
7) Consider the cubic number field $K' = \mathbb{Q}[\alpha]$, where $\alpha^3 = 2$, and let $K'|\mathbb{Q}$ be its Galois hull (i.e., the minimal extension of $K'$ which is Galois over $\mathbb{Q}$).

a) Show that $K = \mathbb{Q}[\zeta, \alpha]$, where $\zeta$ is a primitive 3\textsuperscript{rd} root of 1, and $G = \text{Gal}(K'|\mathbb{Q}) \cong \mathfrak{S}_3$.

b) Detect the decomposition/inertia/ramification groups of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ over rational prime numbers $p < 20$.

c) Is there some $\mathfrak{p}$ such that its decomposition/inertia/ramification group is the whole Galois group $G$?

8) The same questions, correspondingly for the number field $L' = \mathbb{Q}[\alpha], \alpha^3 = 3$, and its Galois hull $L|\mathbb{Q}$.

a) Show that $L = \mathbb{Q}[\alpha, \zeta]$ and that $G = \text{Gal}(L|\mathbb{Q}) = \mathfrak{S}_3$.

b) Answer the questions b) and from 5) in this new situation.

c) Answer the questions c) and from 5) in this new situation.

**Cyclotomic number fields**

9) Let $K_m = \mathbb{Q}[\mu_m]$ be the $m$\textsuperscript{th} cyclotomic number field. Complete the proof of the assertion that $\mathcal{O}_{K_m} = \mathbb{Z}[\mu_m]$ along the lines given in the class:

a) Let $m = p^\omega, \zeta \in \mu_m$ primitive, and $\pi := \zeta - 1$. Then $\pi \in \mathcal{O}_{K_m}$ is a prime element, and $
\mathcal{D}_\zeta = \pi^*$ (what is $\bullet$?).

- Conclude that $\mathcal{O}_{K_m} = \mathbb{Z}[\pi] = \mathbb{Z}[\zeta_m]$ using Dedekind’s Theorem 1.

b) Setting $m = \prod_i m_i, m_i = p_i^{\alpha_i}, m_i' := m/m_i$ with $p_1 < \cdots < p_r$, one has: $\mathcal{D}_{\zeta_m} = \prod \mathcal{D}_{\zeta_{m_i}},$

- and $\mathcal{D}_{\zeta_m} = \prod \mathcal{D}_{\zeta_{m_i}}$.

- Conclude that $\mathcal{O}_{K_m} = \prod_i \mathcal{O}_{K_{m_i}} = \mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_m]$ using the following:

10) Prove the following:

**Proposition.** Let $S'|R, S''|R, S|R$ be extensions of Dedekind rings defined via $L'|K, L''|K$, $L|K$ with $L = L'L''$. Suppose that $\mathcal{D}_{S'|R}, \mathcal{D}_{S''|R}$ are relatively prime in $R$. Prove the following:

a) $\mathcal{D}_{S'|R}, \mathcal{D}_{S''|R}$ are relatively prime in $S$.

b) $S = S'S''$ inside $L$. In particular, the following hold:

$\mathcal{D}_{S|R} = \mathcal{D}_{S'|R} \mathcal{D}_{S''|R} S$, and $\mathcal{D}_{S|R} = \mathcal{D}_{S'|R} \mathcal{D}_{S''|R}$ with $n' := [L' : K], n'' := [L'' : K]$.

11) Describe the decomposition/inertia/ramification groups of the cyclotomic number fields $K_m|\mathbb{Q}$. Try to do the same for the maximal cyclotomic extension $\mathbb{Q}^{\text{cycl}}|\mathbb{Q}$.

[Hint. First describe the cyclotomic character $\chi : \text{Gal}(\mathbb{Q}^{\text{cycl}}|\mathbb{Q}) \to \hat{\mathbb{Z}}^\times$ and then use functoriality.]

**Quadratic residues**

12) Let $p$ be an odd prime number, $\zeta$ a primitive root of unity. Let $S = \sum_{m=1}^{p-1} \left( \frac{m}{p} \right) \zeta^m$ be the Gauß sum attached to the Legendre symbol $\left( \frac{m}{p} \right)$ (WHAT IS THAT?).

Show that $S^2 = \left( \frac{-1}{p} \right) p$. In particular, if $p^* = \left( \frac{-1}{p} \right) p$, then $\sqrt{p^*} \in \mathbb{Z}[\mu_p]$.

13) One defines the **Jacobi Symbol** as follows: Let $m = p_0 p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ be integers such that $p_0 = \pm 1$ and $p_i, q_j$ are prime numbers, $n$ being odd. Suppose that $m$ and
The Jacobi symbol is defined as \( \left( \frac{m}{n} \right)' = \prod_{i,j} \left( \frac{p_i}{q_j} \right) \), where \( \left( \frac{p_i}{q_j} \right) \) is the usual Legendre symbol. Prove the following:

a) If \( m_1 \equiv m_2 \pmod{n} \), then \( \left( \frac{m_1}{n} \right)' = \left( \frac{m_2}{n} \right)' \).

b) \( \left( \frac{m}{n} \right)' \) is multiplicative in both variables \( m \) and \( n \).

c) One has \( \left( \frac{-1}{n} \right)' = (-1)^{(n-1)/2} \). Prove/disprove: \( \left( \frac{2}{n} \right)' = (-1)^{(n^2-1)/8} \).

d) If \( m \) is odd too, then \( \left( \frac{m}{n} \right)' = \left( \frac{n}{m} \right)' \left( \frac{-1}{n} \right)^{(m-1)/2} \left( \frac{-1}{m} \right)^{(n-1)/2} \).

e) Prove or disprove: \( m \pmod{n} \) is a square in \( \mathbb{Z}/n \) iff \( \left( \frac{m}{n} \right)' = 1 \).

Using the properties of the Jacobi symbol try to estimate the number of multiplications needed for checking whether \( x \pmod{p} \) is a square in \( \mathbb{F}_p \). How does this compare with making a list of all the squares in \( \mathbb{F}_p \)?

Deduce the Gauss Reciprocity Law from Problem 13 above.

For a number field \( K \mid \mathbb{Q} \), let \( \text{Div}^\text{ur}(K) \) be the group of divisors of \( \mathcal{O}_K \) which are not ramified over \( \mathbb{Z} \). Describe the Artin map \( (\ , L \mid \mathbb{Q}) : \text{Div}^\text{ur}(K) \to \text{Gal}(K \mid \mathbb{Q}) \) in the following cases:

a) \( K = \mathbb{Q}[\sqrt{d}] \) is a quadratic number field.

b) \( K = \mathbb{Q}[\sqrt{d'}, \sqrt{d''}] \) is a biquadratic number field.

c) \( K = K_n \) is the \( n \)th cyclotomic field.

Question: Which problem concerning primes appears to be related to the Artin map in case c)?