# Sample Algebraic Number Theory Questions

## Thomas R. Shemanske

## June 2007

## 1 Introduction

Graduate students often ask what they should study in preparation for a qualifying exam. The answer is of course that definitions, statements of theorems, examples and sketches of proofs of major theorems are the norm in a qualifying exam. However, this information is often not perceived by the student in the same way as it is intended by the faculty member.

To address this disparity, I have included below a number of sample questions to help you prepare for the algebraic aspect of the number theory qualifying exam. These questions reflect only some of my own prejudices, and are not meant to reflect questions which other examiners might ask. These questions are in no sense intended to reflect a comprehensive review of the material, but should give you a good idea of the type and depth of question which you might be expected to answer. In particular, if you are not comfortable with the vast majority of the material reflected by these questions, you are not ready to take the qual.

In the exam itself, expect to be asked questions like those below, but also some which go beyond the bounds of your knowledge, and possibly outside the bounds of the syllabus. It is by probing the boundaries of your knowledge that we ascertain the depth of your knowledge. You are not expected to know the answer to everything we ask, but you are expected to know a majority.

Caveat: These problems have not really been proofread yet, but I wanted them available ASAP.

## 2 Global Theory

1. Define the ring of integers of a number field. Give a characterization of the ring of integers of quadratic and cyclotomic extensions of $\mathbb{Q}$. Prove the result for quadratic extensions.

2. What is an integral basis? What is the norm of an ideal and why is it finite?

3. Define the terms ramification index and inertia degree. Which primes ramify in quadratic and cyclotomic extensions of $\mathbb{Q}$?

4. Let $L/K$ be an extension of number fields, $\mathfrak{p} \subset \mathcal{O}_K$ a prime. Factor $\mathfrak{p}\mathcal{O}_L$ as a product of primes $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. What is the relation of the $e_i, r$ and $[L : K]$. If $L/K$ is Galois,

how does this affect things and why? Suppose $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. How would you determine the $\mathfrak{P}_i$?

5. Let $p \equiv 1 \pmod 4$ be a prime, and let $K = \mathbb{Q}(\sqrt{p})$. Determine all primes of $\mathbb{Q}$ which ramify in $K$. Determine congruence conditions which describe all primes $q$ which split (completely) in $K$, and congruence conditions for those primes which are inert.

6. Let $p \equiv 1 \pmod 4$ be a prime, $K = \mathbb{Q}(\sqrt{p})$, and $L = \mathbb{Q}(\zeta_p)$ be the $p$th cyclotomic extension. Show that $K \subset L$. Let $q$ be an odd prime which satisfies $q^r \equiv -1 \pmod p$ for some odd positive integer $r$. Determine the factorization (type) of $q\mathcal{O}_K$ and $q\mathcal{O}_L$. How do the primes which occur in the factorization of $q\mathcal{O}_K$ factor in $\mathcal{O}_L$? Work this out explicitly with $p = 13$ and $q = 17$.

7. Let $L/K$ be a Galois extension of number fields, $\mathfrak{p} \subset \mathcal{O}_K$ a prime. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime lying above $\mathfrak{p}$. Describe the decomposition and inertia groups associated to $\mathfrak{p}$ and $\mathfrak{P}$. Determine the order of the decomposition group. If $\mathfrak{P}'$ is another prime of $L$ lying above $\mathfrak{p}$, how are the decomposition groups $D(\mathfrak{P} \mid \mathfrak{p})$ and $D(\mathfrak{P}' \mid \mathfrak{p})$ related? Suppose that $\mathfrak{p}$ is unramified in $L$. Describe how to construct the Frobenius map $\left[\dfrac{L/K}{\mathfrak{P}}\right]$. Show that for abelian extensions, the Frobenius map depends only on $\mathfrak{p}$ and not on $\mathfrak{P}$.

8. Let $K = \mathbb{Q}(\zeta_{13})$, $\mathfrak{p} = 17\mathbb{Z}$, $\mathfrak{P}$ any prime of $K$ lying above $\mathfrak{p}$ and $D$ and $T$ the associated decomposition and inertia groups. Let $K_D$ and $K_T$ be the associated fixed fields. Determine them.

9. Show that $\mathbb{Q}(\sqrt{-5})$ has class number 2 using the Minkowski bound.

# 3   Local Theory

1. Define a valuation on a field. Characterize archimedean and non-archimedean valuations. What are equivalent valuations?

2. What is Ostrowski's theorem?

3. Describe the $p$-adic numbers and integers. Characterize the $p$-adic numbers as Laurent series in $p$. Describe the $p$-adic integers in terms of Laurent series in $p$ and in terms of the $p$-adic valuation on $\mathbb{Q}_p$. Show that $\mathbb{Z}_p$ is a discrete valuation ring. Characterize all the ideals of $\mathbb{Z}_p$.

4. Determine all the archimedean valuations on $\mathbb{Q}(\sqrt[3]{2})$.

5. For an extension of number fields $L/K$ and $\mathfrak{p}$ a prime in $\mathcal{O}_K$, describe the normalized valuation $|\cdot|_{\mathfrak{p}}$ on $K$. Describe all finite extensions of $K_{\mathfrak{p}}$, their valuations, and degrees.

6. Let $p$ be an odd prime in $\mathbb{Z}$. Use Hensel's lemma to prove there are precisely three quadratic extensions of $\mathbb{Q}_p$.