Algebraic number theory (Fall 2013), Homework 1

Frank Thorne, thornef@webmail.sc.edu

Due Friday, January 25

Late homework will be accepted, but more will be posted by next Friday. Remember that you only need 200 points for an A, so you don't have to do all the problems.

Asterisks indicate problems which involve background beyond what is assumed for this course.

1. (5 points) We saw that there is a *local obstruction* to solving the Diophantine equation $x = a^2 + b^2$. It cannot be solved in $\mathbb{Z}/4$, for all $x \in \mathbb{Z}/4$. (Later, we will see that it cannot be solved in $\mathbb{Q}_2$.

   Prove that for any prime p other than 2, and any $x \in \mathbb{Z}/p$, the equation $x = a^2 + b^2$ *can* be solved in $\mathbb{Z}/p$.

2. (5 points) Extending the previous problem, prove further that $x = a^2 + b^2$ can be solved in $\mathbb{Z}/p^c$ for any $p \neq 2$ and any $c \geq 1$, and therefore in $\mathbb{Z}/m$ for any odd m.

   Remark: You may have difficulty proving this; as Dan Kamenetsky pointed out to me, it is false. What can you salvage?

3. (5 points) Suppose that $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Prove carefully that n can be represented as a sum of two squares if and only if each $p_i^{e_i}$ can.

   (We did much of this in lecture, but the 'only if' part was only sketched!)

   Note. A typo was corrected

4. (5 points) Prove that $\sqrt{2} + \sqrt{3}$ generates the biquadratic field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

5. (5 points) Given ring extensions $A \subseteq B \subseteq C$. Suppose that B is integral over A (i.e., every element of B is integral over A) and that C is integral over B. Prove that C is integral over A.

6. (5 points) State the structure theorem for abelian groups. Suppose that $\mathcal{O}_K$ and A are abelian groups, with A a free $\mathbb{Z}$-module. (A free $\mathbb{Z}$-module is defined to be an abelian group that is isomorphic to $\mathbb{Z}^n$ for some n.) Assume further that $\mathcal{O}_K$ and A are contained in a field K, and with $A \subseteq \mathcal{O}_K \subseteq \frac{1}{d}A$. Using the structure theorem, prove that $\mathcal{O}_K$ is also a free $\mathbb{Z}$-module.

7. (5 points) Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Compute $\mathcal{O}_K$. (The answer will depend on D.)

   (You should definitely do this if you have not worked it out before, and even if you have, it is worth a review.)

8. (3 points, *) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Is it the case that $\mathfrak{a}$ must be isomorphic to $\mathcal{O}_K$ as an $\mathcal{O}_K$-module? Is there any condition that would guarantee this?

   (The solution is a tautology; the question is intended to get you used to the vocabulary.)

9. (7 points, *) For a prime power q of your choice, exhibit a quadratic extension $K/\mathbb{F}_q(t)$, and determine its ring of integers (i.e., the integral closure of $\mathbb{F}_q[t]$ in K).

10. (5 points, **) Associate a curve C to your extension, and exhibit an associated map $C \to \mathbb{P}^1(\mathbb{F}_q)$.