Number Theory Fall 2009
Homework 12
Due: Wed. Dec. 2, start of class

10.4 Quadratic fields and their integers

Exercise 10.6. *Let $d \in \mathbb{Z}$ be a non-square. Show that $F = \mathbb{Q}(\sqrt{d})$ has degree 2 over $\mathbb{Q}$.*

Exercise 10.7. *Check that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

Exercise 10.8. *Let d be squarefree, and $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$, i.e., $\alpha \in \mathbb{Q}(\sqrt{d})$. As usual $\overline{\alpha} = a - b\sqrt{d}$, and the norm is $N(\alpha) = \alpha\overline{\alpha}$. Define the* trace *of α to be $\mathrm{tr}(\alpha) = \alpha + \overline{\alpha}$. Show the minimum polynomial for α is $p(x) = x^2 - \mathrm{tr}(\alpha)x + N(\alpha)$.*

This formula may remind you of the formula characterisic polynomial for a 2×2 non-scalar matrix, where one replaces norm by determinant.

In particular this means every $\alpha \in \mathbb{Q}(\sqrt{d})$ is in fact an algebraic number of degree 2. Moreover, it means the integers of $\mathbb{Q}(\sqrt{d})$ are precisely the elements whose trace and norm is an integer. This is a more intuitive way of looking at what it means to be an algebraic integer of degree 2.

Exercise 10.9. *Check the trace (as defined above) is a group homomorphism from $(\mathbb{Q}(\sqrt{d}), +)$ to $(\mathbb{Q}, +)$. In other words check (i) $\mathrm{tr}(\alpha) \in \mathbb{Q}$ for $\alpha \in \mathbb{Q}(\sqrt{d})$, and (ii) $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$ for $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.*

11.1 Revisiting $\mathbb{Z}$

Exercise 11.1. *Check that $\mathcal{I} + \mathcal{J}$ and $\mathcal{I}\mathcal{J}$ indeed define ideals.*

Exercise 11.2. *Let $m, n \in \mathbb{Z}$. Show $(m) + (n) = (\gcd(m, n))$ and $(m)(n) = (mn)$. (Cf. Exercise 11.1.1.)*

Exercise 11.3. *Let R be a ring and $\alpha, \beta \in R$. Show $(\alpha)|(\beta)$ (principal ideals) implies $\alpha|\beta$ (elements). In particular if $R = \mathbb{Z}$ and $m, n \in \mathbb{Z}$, then $(m)|(n) \iff m|n$.*

(I combined Exercise 11.3 and 11.6 from the notes, since the proof is the same.)

11.2 Revisiting $\mathbb{Z}[\sqrt{-3}]$

Exercise 11.4. *Check that the ideal $(2, 1 + \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ is not principal. (Use contradiction.)*

Reading

It may also be a good idea to read over some of Chapter 11 from the text (or the notes) to help familiarize yourself with ideals.

Also, it looks like we won't get around to this in class, so over break why don't you google "Fermat's last theorem n=4." There are several websites that explain the argument, which really isn't so difficult.