Math 154. Homework 1

0. Read the handout on norm and trace, and then do the following calculations.

(*i*) If $K = k(\sqrt{a})$ (nonsquare $a \in k$), for $\alpha = x + y\sqrt{a}$ with $x, y \in k$ show $\mathrm{Tr}_{K/k}(\alpha) = 2x$ and $\mathrm{N}_{K/k}(\alpha) = x^2 - ay^2$.

(*ii*) For the biquadratic field $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $\alpha = x + y\sqrt{2} + z\sqrt{3} + w\sqrt{6} \in K$ with $x, y, z, w \in \mathbf{Q}$, compute $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ and $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ in three ways (as polynomials in x, y, z, w with $\mathbf{Z}$-coefficients): directly use the Galois-theoretic formulas for the norm and trace, use transitivity relative to the tower $K/\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ of quadratic extensions and the general formulas in (*i*), and using instead the tower $K/\mathbf{Q}(\sqrt{3})/\mathbf{Q}$. You should get the same formula in all cases; if not, find your mistake and fix it!

1. Adapting the method of proof of unique factorization for $\mathbf{Z}[\sqrt{-1}]$ from lecture, prove that $\mathbf{Z}[\sqrt{-2}]$ is a unique factorization domain by establishing a division algorithm; the picture of $\mathbf{Z}[\sqrt{-2}]$ as a lattice in the complex plane may be helpful for some insight. Also do the same for $\mathbf{Z}[\sqrt{3}]$ (where there's no geometric picture, just algebra!) by exploiting the inequality $|x^2 - 3y^2| \leq \max(x^2, 3y^2)$ to bypass the lack of a picture.

Where does your argument for $\mathbf{Z}[\sqrt{3}]$ fail to carry over to $\mathbf{Z}[\sqrt{-3}]$ (which we have seen in lecture is not a unique factorization domain)?

2. Using the norm map $\mathbf{Z}[i] \to \mathbf{Z}$, find prime factorizations of $3 + 7i$ and $23 + 14i$.

3. This exercise explores the interference of units when considering pure powers in quadratic rings, but now focusing on squares (when -1 is not a square, in contrast with Fermat's analysis of $y^2 = x^3 - 2$ using cubes in $\mathbf{Z}[\sqrt{-2}]$, for which we got "lucky" in lecture that the units ± 1 were all cubes).

(*i*) Rigorously deduce from the usual definition of a unique factorization domain (i.e., all nonzero nonunits are finite products of irreducible elements, unique up to rearrangement and unit multiplications against the factors) the "pure power" formulation: each nonzero nonunit has the form $\alpha = u\pi_1^{e_1} \cdots \pi_n^{e_n}$ for pairwise non-associate irreducibles π_j and a unit u, and for any other such factorization $\alpha = U\Pi_1^{f_1} \cdots \Pi_N^{f_N}$ necessarily $n = N$ and we can uniquely rearrange the Π_j's so that Π_j is associate to π_j for each j, in which case $e_j = f_j$ for all j. (In other words, the number of factors and the exponents are uniquely determined, up to rearrangement.)

(*ii*) In $\mathbf{Z}[\sqrt{-6}]$ (whose only units are ± 1), observe that $2 \cdot (-3) = (\sqrt{-6})^2$ is a perfect square. Using that $2 - 3 = -1$, show that 2 and -3 have no common irreducible factors. Using the norm map to $\mathbf{Z}$, prove that 2 and -3 are irreducible, and deduce in particular that $\mathbf{Z}[\sqrt{-6}]$ is not a UFD.

(*iii*) In $\mathbf{Z}[\sqrt{6}]$ (which turns out to be a unique factorization domain with infinite unit group: $\pm(5+2\sqrt{6})^{\mathbf{Z}}$, as we'll see later), observe that $2 \cdot 3 = (\sqrt{6})^2$ is a perfect square. Show that 2 and 3 have no common irreducible factors and exhibit each as a *unit multiple* of a square in $\mathbf{Z}[\sqrt{6}]$. (Hint: consider norms, which may be negative, to discover irreducible factorizations for 2 and 3 in $\mathbf{Z}[\sqrt{6}]$. Watch out for associates!)

4. This exercise leads you through an "algebraic number theory" proof of Fermat's two-squares theorem. The result to be shown is that an odd positive prime p has the form $p = x^2 + y^2$ if and only if $p \equiv 1 \bmod 4$. It is assumed that you know that -1 is a square mod p if and only if $p \equiv 1 \bmod 4$.

(*i*) Using mod-4 considerations, show that if p admits such a form then -1 must be a square mod p (and so the case $p \equiv 3 \bmod 4$ is ruled out).

(*ii*) Now assume $p \equiv 1 \bmod 4$, and make $n \in \mathbf{Z}$ so $n^2 \equiv -1 \bmod p$. Since $p|(n^2 + 1)$ in $\mathbf{Z}$, in $\mathbf{Z}[i]$ we have $p|(n + i)(n - i)$. Use this to get a contradiction (via unique factorization) if p is *irreducible* in $\mathbf{Z}[i]$.

(*iii*) By (*ii*), there must be a factorization $p = \alpha\beta$ in $\mathbf{Z}[i]$ with $\alpha, \beta \in \mathbf{Z}[i]$ nonunits. By taking norms of both sides and recalling the explicit formula $\mathrm{N}(u + vi) = u^2 + v^2$ for $u, v \in \mathbf{Q}$, deduce that $p = x^2 + y^2$ for some $x, y \in \mathbf{Z}$.

(*iv*) Adapt this technique with $\mathbf{Z}[\sqrt{-2}]$ to show that if p is an odd positive prime then $p = x^2 + 2y^2$ for some $x, y \in \mathbf{Z}$ if and only if -2 is a square mod p. Using quadratic reciprocity (really the aspect concerning the Legendre symbol $(2|p)$), describe all such p by a congruence condition on p mod 8.