Math 676. Homework 1

1. Prove that $\mathbf{Z}[\sqrt{-1}]$ and $\mathbf{Z}[\sqrt{-2}]$ are Euclidean domains, and likewise for $\mathbf{Z}[\sqrt{2}]$ (so these rings are PID's, and hence they are UFD's). In these examples, use the "absolute norm" $\mathrm{N}(x) = |x\overline{x}|$ as the measure of size for the remainder in the division algorithm.

Also, explain why $\mathbf{Z}[\sqrt{-d}]$ has unit group $\{\pm 1\}$ for squarefree $d \in \mathbf{Z}$ with $d > 1$. (This ring is not always the ring of integers of $\mathbf{Q}(\sqrt{-d})$, but this is not relevant to the determination of its unit group.)

2. (*i*) Prove that $\mathbf{Q}(\zeta_n)$ and $\mathbf{Q}(\zeta_m)$ are isomorphic as abstract fields if and only if $n = m$, $n = 2m$ with m odd, or $m = 2n$ with n odd. (Hint: The problem is equivalent to a literal equality as subfields of a suitable $\mathbf{Q}(\zeta_N)$, and equality of subfields can be studied via Galois theory.)

(*ii*) Find all roots of unity in $\mathbf{Q}(\zeta_n)$, and prove that if K is a number field then K contains only finitely many roots of unity; give a crude bound in terms of $[K : \mathbf{Q}]$.

3. Let A be a domain.

(*i*) Two elements $a, a' \in A$ are *associates* if one of them is a unit multiple of the other (in which case each is a unit multiple of the other). Show that a and a' are associates if and only if the principal ideals aA and $a'A$ coincide.

(*ii*) Prove that A is a UFD if and only if every nonzero principal proper ideal is a product of finitely many principal *prime* ideals such that the set of such primes and their multiplicities is unique up to reordering of the labels.

(*iii*) By Exercise 1, we know that $\mathbf{Z}[\sqrt{2}]$ is a UFD. Use your knowledge concerning Pell's equation to find all units in this ring, and then find a nonzero nonunit $a \in \mathbf{Z}[\sqrt{2}]$ that *cannot* be written in the form $\pm\pi_1^{e_1} \cdots \pi_r^{e_r}$ where the π_i are irreducible and pairwise non-associate. Compare with (*ii*).

(*iv*) If A is a UFD, prove that $A[X]$ is a UFD. For a field k, prove that $k[X, Y]$ is a UFD but not a PID.

4. Let k be a field.

(*i*) Assume that $\mathrm{char}(k) \neq 2$, and let $K/k(X)$ be a quadratic extension (necessarily separable, and even Galois). Show that K is the splitting field of an irreducible polynomial $T^2 - f \in k(X)[T]$ with $f \in k[X]$ a nonzero nonsquare (possibly constant!). In terms of the irreducible factorization of f, compute the integral closure of $k[X]$ in K.

(*ii*) Assume that k has characteristic 2. Let $K/k(X)$ be a *separable* quadratic extension. By Artin-Schreier theory, we know that K is the splitting field of an irreducible polynomial of the form $T^2 - T - f \in k(X)[T]$ with a nonzero $f \in k(X)$ that is unique up to replacing f with $f + (g^2 - g)$ for $g \in k(X)$. Find some obstructions to the possibility of being able to find $f \in k[X]$, and give an explicit such example for $k = \mathbf{F}_2$.

5. Let K be a number field, and let $\mathbf{C}$ denote an algebraic closure of $\mathbf{R}$ (so $[\mathbf{C} : \mathbf{R}] = 2$ and $\mathbf{C}$ is unique up to non-canonical isomorphism). We write $z \mapsto \overline{z}$ to denote the unique non-trivial automorphism of $\mathbf{C}$ over $\mathbf{R}$, and this is called *complex conjugation*.

Since $\mathbf{C}$ is algebraically closed, there are $[K : \mathbf{Q}]$ distinct embeddings $h : K \hookrightarrow \mathbf{C}$. For each such h we write $\overline{h}$ to denote the composite of h with complex conjugation, so $h(K) \subseteq \mathbf{R}$ if and only if $h = \overline{h}$. We say h is *real* if $h(K) \subseteq \mathbf{R}$, and otherwise h is *non-real* (so the non-real embeddings come in conjugate pairs). Let r_1 denote the number of real embeddings and let $2r_2$ be the number of non-real embeddings, so $[K : \mathbf{Q}] = r_1 + 2r_2$.

(*i*) Using the primitive element theorem for $K/\mathbf{Q}$, construct an isomorphism of $\mathbf{R}$-algebras $\mathbf{R} \otimes_{\mathbf{Q}} K \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ (using ring-theoretic product). Can you describe $(\mathbf{R} \otimes_{\mathbf{Q}} K)^{\times}$?

(*ii*) Find an intrinsic meaning (in terms of K) for the indexing set (of size $r_1 + r_2$) that labels the factors in the target of the isomorphism in (*i*).