Math 676, Homework 1

(Turn in solutions to 5 problems.)

1. A *primitive Pythagorean triple* (abbreviated PPT) is a triple $(x, y, z) \in \mathbb{Z}^3$ such that (i) $x^2+y^2=z^2$ and (ii) x, y, and z have no common factors. Classify all such triples, as given in (g), (h) below.

   (a) Show that $\mathbb{Z}[i]$ is a Euclidean domain. See Niven, Zuckerman, Montgomery, Sec. 1.2, 1.3 and generalize the proof for $\mathbb{Z}$).

   (b) Deduce that $\mathbb{Z}[i]$ is a unique factorization domain.

   (c) Show that if (a, b, c) is a PPT, then c must be odd.

   (d) Suppose (a, b, c) is a PPT. Show that if π is a prime element in $\mathbb{Z}[i]$ which divides $(a+ib)$, then π does not divide $(a-ib)$. (Hint: if π divides both, then it divides $2a$. Since π divides the relatively prime numbers c and $2a$, use the fact that $\mathbb{Z}[i]$ is Euclidean to conclude that π divides 1.)

   (e) Conclude that if (a, b, c) is a PPT and π is a prime in $\mathbb{Z}[i]$ which divides $a+ib$, then π^2 divides $a+ib$.

   (f) Note that the units in $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$. From the above, if (a, b, c) is a PPT, then $a+ib = ux^2$ where u is a unit in $\mathbb{Z}[i]$ and $x \in \mathbb{Z}[i]$.

   (g) Show that (a, b, c) is a PPT iff there are relatively prime $m, n \in \mathbb{Z}$ both not odd and $m > 0$ so that $a = (m^2-n^2)$ and $b = 2mn$, or *vice-versa.*

   (h) How unique are n and m?

   (i) (Extra Credit)(*) Classify all solutions to $x^2+y^2+z^2$ with $x, y, z \in \mathbb{Z}[i]$, having no common factors in $\mathbb{Z}[i]$. (The question makes sense since $\mathbb{Z}[i]$ is a UFD.)

2. Prove or disprove:

   (a) The ring $\mathbb{Z}[\frac{1}{2}]$ is integrally closed in its quotient field $\mathbb{Q}$.

   (b) The ring $\mathbb{Z}[\sqrt{5}]$ is integrally closed in its quotient field $\mathbb{Q}(\sqrt{5})$.

3. Let d be a squarefree integer. Show that the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ is:

   (a) $\mathbb{Z}[\sqrt{d}]$ when d is congruent to 2 or 3 mod 4.

   (b) $\mathbb{Z}[(1+\sqrt{d})/2]$ when d is congruent to 1 mod 4.

4. Prove the *Cayley-Hamilton theorem*: Suppose V is an n-dimensional vector space over a field k. Suppose $\{v_1, v_2, \ldots, v_n\}$ is a basis for V. Show that there exist polynomials $p_1, p_2, \ldots, p_n \in \mathbb{Z}[x_{ij}]$ with $1 \leq i, j \leq n$ so that if $T \in \mathrm{End}_k(V)$ is represented by the matrix (T_{ij}) with respect to the basis $\{v_1, v_2, \ldots, v_n\}$, then $T^n + p_1(T_{ij})T^{n-1} + p_2(T_{ij})T^{n-2} + \cdots + p_n(T_{ij}) = 0$. What is $p_1(T_{ij})$?

5. (a) Show that $\{1, 2^{1/3}, 2^{2/3}\}$ is an integral basis of $\mathbb{Q}(2^{1/3})$ (That is, show every element of the ring of integers for $\mathbb{Q}(2^{1/3})$ may be written as a unique integral combination of 1, $2^{1/3}$, and $2^{2/3}$).

   (b) Show that $\{1, \theta, (\theta + \theta^2)/2\}$ is an integral basis for $\mathbb{Q}(\theta)$ where $\theta^3 - \theta = 4$.

6. (Theorem of the primitive element) An algebraic number field $K = \mathbb{Q}(\alpha_1, ..., \alpha_k)$ where each α_j satisfies a polynomial equation over $\mathbb{Q}$. Show that there is an algebraic number β such that $K = \mathbb{Q}(\beta)$, Show that β can be taken to be an algebraic integer. [You should know this result, but please write down a proof.]

7. (a) Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$, and let $\mathbb{A}$ be the integral closure of $\mathbb{Z}$ in $\bar{\mathbb{Q}}$. Prove that for any number field K with ring of integers O_K that $O_K = \mathbb{A} \cap K$.

   (b) Let K, L be algebraic number fields with $K \subset L$ and let B an integrally closed subring of L. Let $A = B \cap K$. Prove or disprove: A is integrally closed in K.

8. Prove that $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ are isomorphic (as abstract fields) if and only if $n = m$ or $n = 2m$ with m odd, or $m = 2n$ with n odd. (Hint: For odd n, consider $-\zeta_{2n}^{n+1} = \zeta_{2n}$. The remainder of the proof requires that you brush up on your Galois theory. One approach is to look at $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ as subfields of some suitable $\mathbb{Q}(\zeta_N)$. Another is to use the fact that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.)

9. (*) Let a *primitive Eulerian triple* be a solution to $x^3 + y^3 = z^3$, with x, y, z in the UFD $\mathbb{Z}[\zeta_6]$ with $\zeta_6 = \frac{1+\sqrt{-3}}{2}]$, and with x, y, z pairwise relatively prime. Show that $xyz = 0$. (This is Fermat's last theorem for $n = 3$. My idea was that you imitate the proof of problem 1 through (f), using $x^3 + y^3 = (x + y)(x - \zeta y)(x - \zeta^5 y)$, and see how far you get, completing argument with infinite descent.)

10. (*) [Problem outside the course] The elements α of a number field K act as endomorphisms E_α on a basis of K as a vector space over $\mathbb{Q}$. If $[K : \mathbb{Q}] = n$ then this action is represented by $n \times n$ matrices (with $\mathbb{Q}$-coefficients); these matrices depend on the basis of K chosen. The endomorphisms $\{E_\alpha : \alpha \in K\}$ form a commutative subalgebra of $M_n(\mathbb{C})$, the ring of $n \times n$ matrices, of dimension n, since it is a ring

isomorphic to K. Prove, in general, that any commutative subalgebra of $M_n(K)$ over a field K containing $\mathbb{Q}$ has dimension at most n: do it for $K = \mathbb{C}$.