Math 316 Homework for Wednesday, Week 2

PROBLEM 1. Prove that $p = x^3 + 2x^2 + 3x + 4$ is irreducible over $\mathbb{Z}$. In other words, if $p = fg$ with $f, g \in \mathbb{Z}[x]$, then one of f or g must be a unit (and the only units in $\mathbb{Z}[x]$ are ± 1). [Hint: a non-trivial factorization of p will have the form $(x - a)(x^2 + bx + c)$ with $a, b, c \in \mathbb{Z}$. Therefore, $p(a) = 0$. So p must have an integer root. Next, if $p(m) = 0$ for some integer m, then $p(m) = 0 \bmod n$ for every integer n. So to show p is irreducible it suffices to find a particular n such that $p(m) = 0 \bmod n$ has no integer solution m—and there are only finitely many values for $m \bmod n$.]

PROBLEM 2. Prove that $1 + i$ is a prime element of $\mathbb{Z}[i]$ by completing the following steps. Let $\alpha = a + bi$ and $\beta = c + di$, and suppose that $(1 + i)|(\alpha\beta)$. We must show that $1 + i$ divides α or β.

(a) Prove that $2|(a^2 + b^2)$ or $2|(c^2 + d^2)$ in $\mathbb{Z}$. (Hint: conjugates.)

(b) Without loss of generality, assume $2|(a^2 + b^2)$. Prove that a and b have the same parity.

(c) Case 1: suppose a and b are both even. Show that $1 + i$ divides $a + bi$.

(d) Case 2: suppose a and b are both odd. Then $a = 2a' + 1$ and $b = 2b' + 1$ for some integers a' and b'. Write $a + bi$ in terms of a' and b' and use this expression to show that $1 + i$ divides $a + bi$.

It turns out that there is a Euclidean algorithm for Guassian integers, which implies—just as it does for $\mathbb{Z}$ and for $K[x]$ when K is a field—that $\mathbb{Z}[i]$ is a PID. Recall that in a PID, primes and irreducibles are the same thing, and it is easy to show $1 + i$ is irreducible. So this would be a more principled way to prove that $1 + i$ is prime in $\mathbb{Z}[i]$. By the way, we have the following interesting fact: for an integer $d < 0$, one may show that $\mathbb{Z}[\sqrt{d}]$ is a PID exactly when d is one of the following:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

PROBLEM 3. Find the minimal polynomial over $\mathbb{Q}$ for each of the following:

(a) $(1 + i)/\sqrt{2}$

(b) $i + \sqrt{2}$

(c) $e^{2\pi i/3} + 2$.

No proof is necessary, but show your work.

Problem 4. Suppose $H \subseteq K \subseteq L$ are fields.

(a) Citing standard results from linear algebra, prove that $[L : H]$ is finite if and only if $[L : K]$ and $[K : H]$ are finite.

(b) Suppose $[L : K]$ is finite. Let $a_1, \cdots, a_s \in L$ be a basis for L/K, and let $b_1, \cdots, b_t \in K$ be a basis for K/H. Prove that $\{a_i b_j\}_{1 \le i \le s, 1 \le j \le t}$ is a basis for L/H and thus show that

$$[L : H] = [L : K][K : H].$$

(Note that both the a_i and the b_j, in addition to being elements of vector spaces, are field elements, and hence can be multiplied together.)

Problem 5. In the following, you may use that fact that if $d \in \mathbb{Z}$, then $\sqrt{d}$ is rational if and only if d is a perfect square. Our main goal is to find, with proof, a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(a) Let d be an integer that is not a perfect square. The field $\mathbb{Q}(\sqrt{d})$ is the smallest field that contains both $\mathbb{Q}$ and $\sqrt{d}$. Its elements have the form

$$\frac{a + b\sqrt{d}}{u + v\sqrt{d}}$$

where $a, b, u, v \in \mathbb{Q}$ and $u + v\sqrt{d} \ne 0$. Prove, without citing results from class, that every such element can be written as $s + t\sqrt{d}$ for some $s, t \in \mathbb{Q}$.

(b) Show that $\{1, \sqrt{d}\}$ is a basis for $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ by giving a direct proof that 1 and $\sqrt{d}$ are linearly independent (they span $\mathbb{Q}(\sqrt{d})$ by the first part of this problem). In other words, if $a + b\sqrt{d} = 0$ for some $a, b \in \mathbb{Q}$, show that $a = b = 0$.

(c) Give a direct proof that 1 and $\sqrt{5}$ are linearly independent over $Q(\sqrt{2})$.

(d) By the previous part of this problem, we have $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}))] \ge 2$. Use Theorem 1.11 to find, with proof, the minimal polynomial for $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}(\sqrt{2})$ and conclude that $[\mathbb{Q}(\sqrt{2}, \sqrt{5} : \mathbb{Q}(\sqrt{2}))] = 2$.

(e) Find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$, i.e., for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ as a vector space over $\mathbb{Q}$.

(f) Write

$$\frac{1}{1 + \sqrt{2} + \sqrt{5}}$$

as a linear combination of your basis elements. Show your work.

Problem 6. Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.