Homework 6 Math 113 Summer 2014.

Due Monday August 4th

Make sure to write your solutions to the following problems in complete English sentences. Solutions that are unreadable or incoherent will receive no credit. Provide complete justifications for all claims that you make. Problems will be of varying difficulty, and do not appear in any order of difficulty. All rings are assumed commutative and with unity.

1. For each of the following ideals, say whether they are prime, maximal (hence also prime), or neither
   (a) $(x^4 + 2x^2 + 1) \subset \mathbb{C}[x]$
   (b) $(x^5 + 24x^3 - 54x^2 + 6x + 12) \subset \mathbb{Q}[x]$
   (c) $(x - a) \subset \mathbb{R}[x, y]$, where $a \in \mathbb{R}$.
   (d) $(4, 2x - 1) \subset \mathbb{Z}[x]$
2. In this problem you will prove a "dictionary" which relates notions of divisibility to principal ideals. Let R be a ring and a, b elements of R.
   (a) Prove that $a|b$ if and only if $b \in (a)$
   (b) Prove that a is a unit if and only if $(a) = R$ (we've used this in class many times)
   (c) Prove that if R is an integral domain, then $a = ub$ for some unit $u \in R$ if and only if $(a) = (b)$.
   (d) Prove that if R is an integral domain and (a) is a nonzero prime ideal, then a is an irreducible element.
   (e) Show, however, by finding an example in $\mathbb{Z}[\sqrt{-5}]$, then even if a is irreducible, the ideal (a) may not be prime[1].
3. Use the division algorithm in $k[x]$ to prove the following lemma, which you might have wished you had for the last HW: If $a \in k$, and a nonconstant linear polynomial f is in the kernel of the evaluation map $\mathrm{Ev}_a \colon k[x] \to k$, then f generates the kernel, so $\ker \mathrm{Ev}_a = (f)$.
4. Prove that any element r in a ring R which is not contained in any maximal ideal must be a unit in R. You may use the following fact: every *nonzero* ring contains a maximal ideal. [Hint: look for a maximal ideal in a suitable quotient, then look at its pre-image under the quotient map. Is it maximal?]
5. Let R be a ring, and $\mathfrak{n}$ the set of nilpotent elements in R.
   (a) Prove that $\mathfrak{n}$ is an ideal (remember that we allow 0 as a nilpotent).
   (b) Prove that $\mathfrak{n}$ is contained inside every prime ideal of R.
   (c) Prove that the ring $R/\mathfrak{n}$ has no nonzero nilpotent elements.
6. The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, with norm $n \colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ given by $n(a+bi) = a^2+b^2$ (you don't need to prove that this makes $\mathbb{Z}[i]$ into a Euclidean domain).
   (a) Show that this norm satisfies the stronger condition $n(\alpha\beta) = n(\alpha)n(\beta)$

[1] This can only happen when the ring is *not* a UFD.

(b) Deduce that if $\alpha|\beta$ in $\mathbb{Z}[i]$, then $n(\alpha)|n(\beta)$ in $\mathbb{N}$.

(c) Show that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $n(\alpha) = 1$. Use this to determine all the units in $\mathbb{Z}[i]$.

(d) Show that if $n(\alpha)$ is a prime in $\mathbb{N}$, then α is irreducible in $\mathbb{Z}[i]$.

(e) Why don't the equalities $(4+i)(4-i) = 17 = (1+4i)(1-4i)$ contradict the fact that $\mathbb{Z}[i]$ is a UFD (this follows from the fact that it's a Euclidean domain)?

7. Let $R = k[[x]]$ be the ring of formal power series over a field k.

(a) Prove that the ideal (x) generated by x is maximal, by looking at the quotient $R/(x)$.

(b) In fact, this is the *only* maximal ideal of R. Use this and problem 4 to give a new proof of the worksheet problem from last week which said that the units in R are those power series with nonzero constant term, i.e., those $\sum a_i x^i$ for which $a_0 \neq 0$.

8. By definition, the **content** of a polynomial $f \in \mathbb{Z}[x]$, written $C(f)$, is the gcd of its coefficients. Prove **Gauss' Lemma**, which states that for $f, g \in \mathbb{Z}[x]$, $C(fg) = C(f)C(g)$. [Hint: First factor out the content from each polynomial, and reduce to the case where f and g both have content 1: in this case you have to prove that $C(fg) = 1$. Now argue by contradiction, supposing some prime p divides all coefficients of fg, and looking at their reduction mod p, as we did in the proof of Eisenstein's criterion.]

9. Use Gauss' Lemma to prove that if $f \in \mathbb{Z}[x]$ and $C(f) = 1$, then f is irreducible over $\mathbb{Z}$ if and only if f is irreducible over $\mathbb{Q}$.

10. In this problem you will investigate the behavior of prime ideals under a ring homomorphism $f: R \to S$. First, a definition: if $I \subseteq R$ is an ideal, the **extension** of I across f is the ideal $I^e = (f(I))$ generated by $f(I)$. In other words, it consists of all elements of the form $\sum s_i f(r_i)$, for $r_i \in R$, $s_i \in S$.

(a) Prove that if $J \subseteq S$ is an ideal, then the pre-image $f^{-1}(J)$ is an ideal in R. Prove further that if J is prime, so is $f^{-1}(J)$. This says that "primes pull back".

(b) Show by giving an example that if $I \subseteq R$ is an ideal, then $f(I)$ is not necessarily an ideal (this is the reason why we define the extension of an ideal - it's the smallest ideal containing the image of I)

(c) Now let $f: \mathbb{Z} \to \mathbb{Z}[i]$ be the inclusion of the usual integers into the Gaussian integers. Let p be a prime, and (p) the ideal it generates in $\mathbb{Z}$. In this case the extension $(p)^e$ is just the ideal generated by the (usual) integer p in the ring $\mathbb{Z}[i]$ (note this will be much larger than the ideal (p) in $\mathbb{Z}$). Prove the following facts:

i. If $p = 2$, then $(p)^e$ is the same as the ideal generated by $(1+i)^2$, which is not prime.

ii. If $p \equiv 1 \mod 4$, then $(p)^e$ is not a prime ideal in $\mathbb{Z}[i]$.

iii. If $p \equiv 3 \mod 4$, then $(p)^e$ is a prime ideal in $\mathbb{Z}[i]$

These examples show that extensions of primes need not be prime, or "primes do not push forward". In proving ii and iii, you may use the following famous theorem of Fermat: a prime $p > 2$ can be written as $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$