Homework 7, Math 701 – Frank Thorne (thorne@math.sc.edu)

Instructions: You are welcome and encouraged to collaborate, but please write up your own solutions.

Due Friday, December 8, 2017.

1. Let $R = \mathbb{Z}[\sqrt{-n}]$, where n is a squarefree integer ≥ 3.
   (a) Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducible in R.
   (b) Prove that R is not a UFD. (For example, one may prove that any one of the above irreducible elements is not prime.)
   (c) Give an explicit ideal in R that is not principal.

2. Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$. Prove that the quotient ring $\mathbb{Z}[i]/(\alpha)$ has exactly $a^2 + b^2$ distinct elements.

   Here is one way in which this may be proved. (Feel free to vary as you see fit.)
   (a) Use the Chinese remainder theorem to reduce to the case where $\alpha = \pi^n$ is a power of a prime element π of $\mathbb{Z}[i]$.
   (b) Explain why multiplication by π^n induces a $\mathbb{Z}[i]$-module homomorphism $\mathbb{Z}[i]/\pi^{n+1}\mathbb{Z}[i] \to \mathbb{Z}[i]/\pi^{n+1}\mathbb{Z}[i]$. Compute its image and kernel. Writing $|M|$ for the number of elements in a module M, prove (by induction) that $|\mathbb{Z}[i]/\pi^n\mathbb{Z}[i]| = |\mathbb{Z}[i]/\pi\mathbb{Z}[i]|^n$.
   (c) Prove the result in the case where π is prime, and conclude.

3. Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.
   (a) Prove that R is an integral domain and that its units are ± 1.
   (b) Show that the irreducibles in R are $\pm p$ for primes $p \in \mathbb{Z}$, and polynomials f which are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.
   (c) Show that x cannot be written as the product of irreducibles in R (and, in particular, that x is not irreducible), and hence that R is not a UFD.
   (d) Show that x is not prime in R and describe the quotient ring $R/(x)$.

4. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

5. Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules.

6. Let N be a submodule of a module M. Prove that if M/N and N are both finitely generated, then so is M.