6370-001 - FALL 2021 - WEEK 1 (8/24, 8/26)

Exercise 1.

(1) Compute some examples to come up with a conjecture about which odd primes p are expressible as $p = a^2 + b^2$ for integers a and b.
(2) Prove your conjecture by computing $\mathbb{Z}[i]/(p)$ in two different ways.
(Hint: for one way, you will want to use that $\mathbb{Z}[i]$ is a UFD and the norm map $z = x + iy \mapsto |z|^2 = z\overline{z} = x^2 + y^2$. For the other, use $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$).

Exercise 2.
Give an elementary proof that p is a square mod 3 if and only if -3 is a square mod p (hint: $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$.)

Exercise 3.

(1) Let K be a field of characteristic not equal to 2. Give an elementary proof that every quadratic extension of K is generated by a square-root of an element in K. What happens in characteristic two?
(2) For $k, k' \in K$, when is $K[x]/(x^2 - k) \cong K[x]/(x^2 - k')$ (as K-algebras)?
(3) For $k \in \mathbb{Z}$ squarefree, which elements of $\mathbb{Q}(\pm\sqrt{k})$ have minimal polynomial with integer coefficients?
(4) For $f(t) \in \mathbb{F}_q[t]$ squarefree, which elements of the field $\mathbb{F}_q(t)[x]/(x^2 - f(t))$ have minimal polynomial with coefficients in $\mathbb{F}_q[t]$?

Exercise 4.

(1) If K is a field and $k_0, k_1, \ldots, k_n$ are distinct elements of K and $c_0, c_1, \ldots, c_n$ are any elements of K, construct a polynomial $f(x) \in K[x]$ of degree $\leq n$ with such that $f(k_i) = c_i \; \forall 0 \leq i \leq n$.
(2) What does this have to do with the Chinese Remainder Theorem? (If you don't know/remember it, recall the statement and proof of the CRT in a general commutative ring, e.g. from Chapter 1 of Milne's notes).
(3) Suppose $f(x) \in \mathbb{Q}[x]$ is such that $f(k) \in \mathbb{Z}$ for all $k \in Z$. Is $f \in \mathbb{Z}[x]$?
(4) Use (1) to describe an algorithm for factoring polynomials in $\mathbb{Q}[x]$.

Exercise 5.
Which elements are invertible in $R[[t]]$, the power series ring in one variable with coefficients in R?

Exercise 6.
Show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\mu_3]$ are Euclidean domains (thus, in particular, PIDs (thus, in particular, UFDs)).