Homework #10.

Plan for next week: Finite fields (9.5 + some other stuff), Hilbert basis theorem (9.6).

Problems, to be submitted by Tuesday, November, 22nd

1. Let $R = \mathbb{Z} + x\mathbb{Q}[x]$, the subring of $\mathbb{Q}[x]$ consisting of polynomials whose constant term is an integer.
(a) Show that the element αx, with $\alpha \in \mathbb{Q}$ is NOT irreducible in R. Deduce that x cannot be written as a product of irreducibles in R. Note that by Proposition 21.4 this implies that R is not Noetherian.
(b) Now prove directly that R is not Noetherian by showing that $I = x\mathbb{Q}[x]$ is an ideal of R which is not finitely generated.
(c) Give an example of a non-Noetherian domain which is a UFD.

2. Give an example of a domain R (other than a field or the zero ring) which has no irreducible elements. **Hint:** Start with the ring of power series $R = F[[x]]$ where F is a field. Then up to associates x is the only irreducible element of R. Construct a larger ring $R_1 \supseteq R$ s.t. x is reducible in R_1, but $R_1 \cong F[[x]]$. Then iterating the process construct an infinite ascending chain $R \subseteq R_1 \subseteq R_2 \subseteq \ldots$ and consider its union.

3. (a) Let R be a domain and let $f \in R$. Prove that f is irreducible in R if and only if f is irreducible in $R[x]$.

(b) Recall the main theorem of Lecture 22: *If R is a UFD, then $R[x]$ is a UFD.* This exercises provides an alternative proof for the uniqueness of factorization in $R[x]$.
So, assume that R is a UFD. Recall that by Proposition 21.5 factorization into irreducibles in a commutative domain S with 1 is at most unique whenever every irreducible element of S is prime. Thus, it is enough to show that every irreducible element of $R[x]$ is prime in $R[x]$. So, let p be an irreducible element of $R[x]$. Consider two cases:
Case 1: p is a constant polynomial, that is $p \in R$. Show that $R[x]/pR[x] \cong R/pR$ and use this isomorphism to prove that p is prime in $R[x]$.
Case 2: p is a non-constant polynomial. In this case one can prove that p is prime in $R[x]$ via the following chain of implications, where F denotes the field of fractions of R:

f is irreducible in $R[x] \Rightarrow p$ is irreducible in $F[x] \Rightarrow p$ is prime in $F[x] \Rightarrow p$ is prime in $R[x]$
The first two of these implications easily follow from things we proved in class. The third one can be proved similarly to Gauss lemma.

4. Let F be a field, take $f(x,y) \in F[x,y]$, and write $f(x,y) = \sum_{i=0}^{n} c_i(y)x^i$ where $c_i(y) \in F[y]$. Suppose that

(i) There exists $\alpha \in F$ such that $c_n(\alpha) \neq 0$

(ii) $gcd(c_0(y), c_1(y), \ldots, c_n(y)) = 1$ in $F[y]$

(iii) $f(x,\alpha)$ is an irreducible element of $F[x]$ (where $f(x,\alpha)$ is the polynomial obtained from $f(x,y)$ be substituting α for y).

Prove that $f(x,y)$ is irreducible in $F[x,y]$.

5. Prove that the following polynomials are irreducible:
(a) $f(x,y) = y^3 + x^2y^2 + x^3y + x^2 + x$ in $\mathbb{Q}[x,y]$
(b) $f(x,y) = xy^2 + x^2y + 2xy + x + y + 1$ in $\mathbb{Q}[x,y]$
(c) $f(x) = x^5 - 3x^2 + 15x - 7$ in $\mathbb{Q}[x]$

Hint for (c): By Gauss Lemma, it is enough to prove irreducibility of $f(x)$ in $\mathbb{Z}[x]$. Consider the reduction map $u(x) \to \overline{u}(x)$ from $\mathbb{Z}[x]$ to $\mathbb{Z}_3[x]$, consider possible factorizations of $\overline{f}(x)$ and show that none of them can be lifted to a factorization of $f(x)$ (the general idea is similar to the proof of the Eisenstein criterion).

6. Let p be a prime. Use direct counting argument to find the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ for $n = 2, 3, 4$ and check that your answer matches the general formula derived in the online supplement (to be posted). **Hint:** The number of irreducible monic polynomials of degree n equals the total number of monic polynomials of degree n minus the number of reducible monic polynomials of degree n; the latter can be computed consdering possible factorizations into irreducibles (assuming the number of irreducible monic polynomials of degree m for $m < n$ has already been computed).