Homework #10.

Plan for next three classes:

Tuesday, November 17th: Irreducibility criteria in polynomial rings (9.4);
Thursday, November 19th: Finite fields (9.5 + some other stuff)
Thursday, November 24th: Local rings (no specific section in DF)

1. The following exercises are related to the material that will be discussed in class on Thu, Nov 19th and Tue, Nov, 24th. It is not necessary to write down the solutions, but you should at least sketch the proofs.
(a) (by Thu, Nov 19th) DF, Problems 7.2.3 and 7.2.5
(b) (by Thu, Nov 19th) Let M be an ideal of a commutative ring R with 1. Prove that the following conditions are equivalent:
(i) M is the unique maximal ideal of R
(ii) every element of $R \setminus M$ is invertible.
A commutative ring with 1 which has the unique maximal ideal is called *local*.
(c) (by Tue, Nov 24th) (a) DF, Problem 7.1.26 and 7.1.27

Part A: To be submitted by Thursday, November, 19th

2. $R = \mathbb{Z} + x\mathbb{Q}[x]$, 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 22.3 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.

3. 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 $F[[x]]$ where F is a field, and enlarge it in a suitable way.

4. (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 23: *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 22.4 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.

Part B: to be submitted by Tuesday, November, 24th

5. 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 $F[x,y]$.

6. 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 $\mathbb{Q}[x]$

7. 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).