30) a) Consider the polynomial $f(x) = x^4 + 1 \in \mathbb{Z}[x]$. Evaluate $g(x) := f(x+1)$ and show using Eisenstein's criterion that $g(x)$ is irreducible. Conclude that $f(x)$ is irreducible.
b) For a prime p let

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

the *p-th cyclotomic polynomial*. Show, as in a) that $\Phi_p(x)$ is irreducible.

31) Let F be a field and $f, g \in F[x,y]$. Suppose that (x_0, y_0) is a common solution to $f(x,y) = 0$, $g(x,y) = 0$.
a) Show that y_0 must be a root of $\mathrm{Res}_x(f(x,y), g(x,y))$.
b) Describe a method, based on a), that solves a system of polynomial equations by first eliminating all variables but one using resultants, then solves this polynomial in one variable, and finally uses back-substitution to find all solutions.
c) Use the method of b) to find all rational solution to the following system of equations:

$$\{x^2y - 3xy^2 + x^2 - 3xy = 0, x^3y + x^3 - 4y^2 - 3y + 1 = 0\}$$

32) Let R be an integral domain and F the algebraic closure of its quotient field. $f(x), g(x) \in R[x]$. Suppose that $\alpha, \beta \in F$ such that $f(\alpha) = 0$, $g(\beta) = 0$.
a) Show that $\mathrm{Res}(f(x-y), g(y), y)$ has a root $\alpha + \beta$. (Note: Similar expressions exist for $\alpha - \beta$, $\alpha \cdot \beta$ and α/β.)
b) Construct a polynomial $f \in \mathbb{Q}[x]$ such that $f(\sqrt{5} + \sqrt[3]{2}) = 0$.

33) Let F be a field. For a polynomial

$$f = \sum_{i=0}^{n} a_i x^i \in F[x]$$

we define the *derivative* Df as

$$Df = \sum_{i=1}^{n} i \cdot a_i x^{i-1}$$

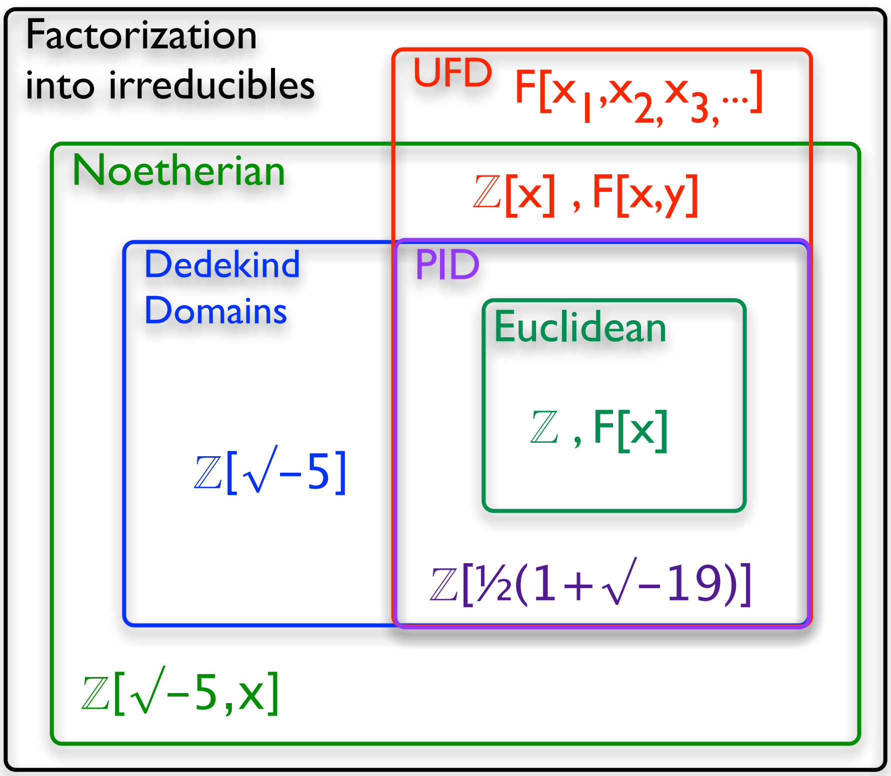
(with i being the the corresponding sum of 1s.)
a) Show that for $f, g \in F[x]$ we have that $D(fg) = (Df)g + f(Dg)$.
b) Suppose that $f = a_n \prod (x - \alpha_i)$ in F. Show that f has roots with multiplicity > 1 if and only if f and Df have a nonconstant gcd.
c) The *discriminant* of a polynomial $f \in F[x]$ of degree m with leading coefficient a is defined as

$$\mathrm{Disc}(f) = (-1)^{\frac{m(m-1)}{2}} \mathrm{Res}(f, Df)/a.$$

Show that $\mathrm{Disc}(f) = 0$ if and only if f has roots with multiplicity > 1 (possibly in a larger field than F).
d) Show that if $f = \prod_i (x - \alpha_i)$, we have that $\mathrm{Disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$.

34) a) Let $f(x) \in \mathbb{Z}[x]$ be irreducible. Show that there are only finitely many primes p, such that the reduction of f modulo p has multiple roots. (Hint: Discriminant)
b) Determine all such primes for the polynomial $x^7 + 15x^6 + 12$.

Classes of Integral Domains



F is a field

UFD: irreducibles are prime, gcd exists
PID: gcd can be expressed in the form xa+yb
Euclidean: gcd can be computed with the euclidean algorithm
Dedekind Domain: Every Ideal is a product of prime ideals (Rings of algebraic integers in a field extension are Dedekind domains)