McGill University
Math 371B: Algebra IV
Solution Sheet for Assignment 2

1. If a, b are elements of a commutative ring with unity then ab is invertible iff a and b are invertible. Use this to show that the non-invertible elements of a valuation ring A are a maximal ideal. The most difficult thing to show is that the sum of non-invertible elements $a, b \neq 0$ is non-invertible. For this, use the fact that $a + b = a(1 + b/a) = b(1 + a/b)$ and the fact that one of a/b, b/a is in A.

   The localization B of $F[x, y]$ with respect to (x, y) consists of those fractions f/g with $f, g \in F[x, y]$ and $f(0, 0) \neq 0$. Neither the element x/y nor its inverse y/x is in B since $xg = yf$ implies that $f, g \in (x, y)$.

2. If A is a discrete valuation ring and $v(p) = 1$ then any non-zero element $a \in A$ can be uniquely written in the form $a = up^n$ with $u \in A^\times,\ n \in \mathbb{N}$. From this it follows that the non zero ideals of A are the ideals (p^n). Conversely, if A is a PID with a single non-zero maximal ideal (p), it suffices to show that every element $a \in A$ can be written in the form $a = up^n$ with $p \not| u$. If this were false, one could find a strictly increasing chain of ideals (a_i) which is not possible in a PID.

   If A is a discrete valuation ring with quotient field K and V is valuation ring of K with $A \subset V$, we have to show $V = K$. We use the fact that every non-zero element of K is of the form up^n with u a unit of A, p a generator of the maximal ideal of A and $n \in \mathbb{Z}$. An element of V not in A must have the form up^{-n} with $n \geq 1$. This implies that $p^{-n} \in V$. But $p^n \in V$ implies that p^n, and hence p, is invertible in V which implies that $V = B$. Since we did not use the hypothesis that V was a valuation ring of K, we have actually shown that a discrete valuation ring is a maximal subring of its quotient field.

3. Let V be a non-trivial valuation ring of $\mathbb{Q}$ and let M be its maximal ideal. Then $M \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and is non-zero; otherwise, the non-zero integers would be invertible in V contradicting $V \neq \mathbb{Q}$. If $M \cap \mathbb{Z} = (p)$ then $A_{(p)} \subseteq V$ which implies that $V = A_{(p)}$ since $A_{(p)}$ is a discrete valuation ring.

4. Let V be a non-trivial valuation ring of $F(x)$. We have either $x \in V$ or $1/x \in V$ and so V contains $F[x]$ or $F[1/x]$. We also have $F[x] \cong F[1/x]$ and $F(x)$ is also the quotient field of $F[1/x]$. If M is the maximal ideal of V and V contains $F[x]$ then $M \cap F[x]$ is a non-zero prime ideal $(p(x))$ with $p(x)$ an irreducible polynomial in $F[x]$. Since V contains the discrete valuation ring $F[x]_{(p(x))}$. It follows that $V = F[x]_{(p(x))}$. If V contains $F[1/x]$ then, as above $V = F[1/x]_{(p(1/x))}$ with p an irreducible polynomial in $F[x]$. If $p(x) \neq x$ we have $F[x]_{(p(x))} = F[1/x]_{(p^*(1/x))}$, where $p^* = x^{\deg(p)}p(1/x)$. If $p(x) = x$ then $F[1/x]_{(1/x)} \neq F[x]_{(x)}$; if $f = a_m x^m + \ldots + a_n x^n$ with $a_m, a_n \neq 0$ we have $v_x(f) = m$ and $v_{1/x}(f) = -n$

5. (a) If $p_1(x), \ldots p_n(x)$ are irreducible then any irreducible factor of $p_1(x)p_2(x) \cdots p_n(x) + 1$ is not an associate of $p_1(x), \ldots p_n(x)$.

   (b) Let $p_1, p_2, \ldots p_n$ be primes of $\mathbb{Z}$ and let S be the set of those integers not divisible by these primes. Then S is a multiplicative subset of $\mathbb{Z}$ and $S^{-1}\mathbb{Z}$ is a ring with n primes (up to associates). The only PID with finitely many primes (not identifying associates) is a field. **Proof by Chiu Fan Lee:** If $p_1, \ldots, p_n$ are the only primes and $n \geq 1$ let $q = p_1 \ldots p_n$. Then the elements of the form $q^k + 1$ are distinct units for $k \geq 1$. This means that the group of units is infinite and hence that the number of primes is infinite which contradicts our assumption.