January 25, 2013
Galois theory

**1. Theorem.**

(1) *If $R$ is UFD, then a non zero element in $R$is prime if and only if it is irreducible.*
(2) *If $R$ is UFD, then $R[X]$ is UFD.*
(3) *If $R$ is PID, then $R$ is UFD.*
(4) *$R[X]$ is PID if and only if $R$ is a field.*

We will only show statement (3). Statement (1) is a consequence of so called Gauss Lemma. Statement (2) is a good exercise.

Assume first that $R$ is a field. Recall that under this assumption for any $f$ in $R[X]$ and any nonzero $g$ in $R[X]$, $f$ can be written in a unique watt as $f = hg + r$ where $\deg(r) < \deg(g)$. Let $I$be an ideal in $R[X]$. If $I$ is the zero ideal then $I = (0)$ is generated by one element. If $I$ is non-zero, let $g$ in $I$ be a non-zero element with the smallest degree. For any $f$ in $I$, we can then write $f = hg + r$. Since both $f$ and $g$ are in $I$, then so is $r = f - hg$. Since $\deg(r) < \deg(g)$, we then must have $r = 0$ and hence $g|f$. This means that $I = (g)$ and so $I$is singly generated.

Assume that $R[X]$ is a PID. Let $r$ in $R$ be non-zero. We need to show that $r$ is invertible, i.e., the ideal in $R$ generated by $r$ is $R$. Let $s$ be in $R$. Note that the ideal $(s)$ in $R[X]$ generated by $s$ consists of all the polynomials whose coefficients are divisible by $s$. Consider then the set $I$ which consists of all polynomials $a_0 + a_1X + \cdots a_kX^k$ such that $r$ divides $a_0$. This is an ideal. And since $R[X]$ is a PID, there is $f$ such that $I = (f)$. As $r$ is in $I$, then $f|r$. It follows then that the degree of $f$ is 0 and hence it is an element of $R$. Thus $r|f$ and so $I = (f) = (r)$. However the ideal $(r)$ consists only of polynomials whose all coefficients are divisible by $r$. It follows that $r$ devices all elements in $R$, i.e., $r$ is invertible.

**2. Proposition.** *Let $R$ be a PID and $r$ be a prime element in $R$ which is non-zero. Then $R/(r)$ is a field.*

Let $s + (r)$ be a non-zero element in $R/(r)$. This means that $s$ does note belong to $(r)$, i.e., $r$ does not divide $s$. Consider the ideal $(r, s)$ in $R$. Since $R$ is PID, there is $t$ such that $(r, s) = (t)$. In particular $t|s$ and $t|r$. We can then write $r = tr'$. Note that $r$ can not divide $t$ since then $r$ would divide $s$ as $t$ does. Hence since $r$ is prime, $r$ devices $r'$. We thus have an equality $r = trr''$. As $R$ is a domain we then get $1 = tr''$. The element $t$ is then invertible and so $(r, s) = (t) = R$. Ion particular there are elements $a$ and $b$ in $R$ so that $ar + bs = 1$. This means that $b + (r)$ is the inverse of $s + (r)$ in $R/(r)$ and so this quaint ring is a field

**3.** Here we will recall the construction of the field of fractions of a domain. Let $R$ be a domain. Consider the set of pairs $(a, b)$ of elements of $R$ with $b \neq 0$. We say that two such pairs $(a, b)$ and $(c, d)$ are equivalent if $ad = bc$. This is an equivalence relation on the set of such pairs. An equivalence class of a pair $(a, b)$ is denoted by $\frac{a}{b}$ and called a fraction. Thus $\frac{a}{b} = \frac{c}{d}$ if $ad = bc$. The set of equivalence classes of this relation is denoted by $K$. This set together with the elements $\frac{0}{1}$ as the zero, $\frac{1}{1}$ as the one, and operations $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ and $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$ is a field, called the field of fractions of $R$. We will identify $R$ with a subring of $K$ given by the fractions $\frac{r}{1}$.

4. **Eisenstein's criterion.** Let $R$ be a UFD and $K$ its ring of fractions. Consider a polynomial $f = a_0 + a_1X + \cdots + a_nX^n$ in $R[X] \subset K[X]$. Assume that there is a prime element $p$ in $R$ such that $p \not| a_n$, $p|a_i$ for $0 \le i < n$ and $p^2 \not| a_0$. Then $f$ is irreducible in $K[X]$.

5. Let $F$ be a field. Then $F[X]$ is a PID and hence UFD. It follows that a non-zero prime polynomial in $F[X]$ is prime if and only if it is irreducible. Thus we will use in this case the words prime polynomial and irreducible polynomial interchangeably.

Let $R$ be a UFD and $K$ its ring of fractions. Consider a polynomial $f = a_0 + a_1X + \cdots + a_nX^n$ in $R[X] \subset K[X]$. Assume that there is a prime element $p$ in $R$ such that $p \not| a_n$, $p|a_i$ for $0 \le i < n$ and $p^2 \not| a_0$. Then $f$ is irreducible in $K[X]$.