Lemma 3.1

Dan Richmond, Jolie Roat

IMMERSE 2009, UNL

July, 2009
Lemma 3.1

Assume there is a (nontrivial) discrete valuation $\nu$ on $K$ and an ideal $\mu$ of $D$ such that $D/\mu$ is finite. Then, for every integer $n \geq 1$, there exists a product of $q$ irreducible elements of $\text{Int}(D)$ with values in $\mu^n$, where $q$ is the cardinal of $D/\mu$. 
Discrete Valuation

Definition
Let $G$ be a group isomorphic to $\mathbb{Z}$. A discrete valuation on a field $K$ is a function $\nu : K^* \rightarrow G$ satisfying

- $\nu$ is surjective
- $\nu(xy) = \nu(x) + \nu(y)$, for all $x, y \in K^*$
- $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, for all $x, y \in K^*$ with $x + y \neq 0$. 

Show $\exists b \in \mu$ such that $\nu(b) \neq 0$
Outline

1. Show $\exists b \in \mu$ such that $\nu(b) \neq 0$
2. Construct a set of irreducible polynomials $f_i \in \text{Int}(D)$
1. Show $\exists b \in \mu$ such that $\nu(b) \neq 0$

2. Construct a set of irreducible polynomials $f_i \in \text{Int}(D)$

3. Prove for every $\alpha \in D$

$$\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n.$$ 

where $q$ is the cardinal of $D/\mu$
Show $\exists b \in \mu$ such that $\nu(b) \neq 0$

Proof.

Since $\nu$ is nontrivial, $\exists x \in D$ such that $\nu(x) \neq 0$. Then, let $y \in \mu$.

- Case 1: $\nu(y) \neq 0$. Then take $b = y$. 

Show $\exists b \in \mu$ such that $\nu(b) \neq 0$

Proof.

Since $\nu$ is nontrivial, $\exists x \in D$ such that $\nu(x) \neq 0$. Then, let $y \in \mu$.

- Case 1: $\nu(y) \neq 0$. Then take $b = y$.
- Case 2: $\nu(y) = 0$. Let $b = xy$. Then,

$$\nu(b) = \nu(xy) = \nu(x) + \nu(y) = \nu(x) + 0$$

Then, $\nu(x) \neq 0$, so $\nu(b) \neq 0$ and $b = xy \in \mu$ by the definition of an ideal.
Construct a set of irreducible polynomials $f_i \in \text{Int}(D)$

**Proof.**

Let $u_0, u_1, \ldots, u_{q-1}$ be representatives of $D/\mu$.
Consider $m$ to be an integer prime to $n\nu(b)$.

**Note:**

\[
    n\nu(b) = \nu(b) + \nu(b) + \ldots + \nu(b) = \nu(b^n)
\]

Hence, $m$ is an integer prime to $\nu(b^n)$ so by Proposition 2.7, the polynomials $f_i = (X - u_i)^m + b^n$ are irreducible in $\text{Int}(D)$. \qed
Prove for every $\alpha \in D$, $\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n$.

Proof.
Consider $m > n$. Then, $\forall \alpha \in D$, $\exists i$ where $1 \leq i \leq q - 1$ such that $(\alpha - u_i) \in \mu$. 
Prove for every $\alpha \in D$, $\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n$.

Proof.

Consider $m > n$. Then, $\forall \alpha \in D$, $\exists i$ where $1 \leq i \leq q - 1$ such that $(\alpha - u_i) \in \mu$. Then,

$$f_i(\alpha) = (\alpha - u_i)^m + b^n$$
Prove for every $\alpha \in D$, $\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n$.

Proof.

Consider $m > n$. Then, $\forall \alpha \in D$, $\exists i$ where $1 \leq i \leq q - 1$ such that $(\alpha - u_i) \in \mu$. Then,

$$f_i(\alpha) = (\alpha - u_i)^m + b^n = (\alpha - u_i)^n(\alpha - u_i)^{m-n} + b^n \in \mu^n$$

Hence, for every $\alpha \in D$, there exists an $i$ such that $f_i(\alpha) \in \mu^n$. 
Prove for every $\alpha \in D$, $\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n$.

Proof.

Consider $m > n$. Then, $\forall \alpha \in D$, $\exists i$ where $1 \leq i \leq q - 1$ such that $(\alpha - u_i) \in \mu$. Then,

$$f_i(\alpha) = (\alpha - u_i)^m + b^n = (\alpha - u_i)^n(\alpha - u_i)^{m-n} + b^n \in \mu^n$$

Hence, for every $\alpha \in D$, there exists an $i$ such that $f_i(\alpha) \in \mu^n$. Then, $\prod_{i=0}^{q-1} f_i = f_0 \ldots f_{q-1}$.

By definition of ideal, for every $\alpha \in D$

$$\prod_{i=0}^{q-1} f_i(\alpha) \in \mu^n.$$