Explicit Factorization in Dedekind Domains Obtained via a Monic Polynomial

In this unit we'll show how to factor ideals under certain fairly general conditions on the ring in question.

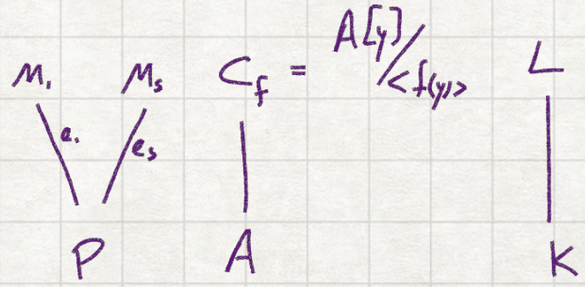
Let A D.D. $f(y) \in A[y]$ monic & irr with $\deg f = n$. Denote as usual $C_f = A[y]/\langle f(y) \rangle$.

$K = \operatorname{Frac} A$, $L = \operatorname{Frac} C_f$ (note that f irr $\Rightarrow C_f$ domain and so L is well-defined).

Since f is irr in $A[y]$ and so in $K[y]$, $[L:K] = \deg f = n$.

As f is monic, C_f is integral over A. However, it is not necessarily the integral closure of A in L (e.g., the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is not always just $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[y]/\langle y^2 - d \rangle$. Indeed, when $d \neq 1$ square-free with $d \equiv_4 1$, the i.c. of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$).

In this unit we'll show how to factor PC_f where $P \in \operatorname{Max} A$, A D.D, assuming C_f is D.D.



Remark

In the study of algebraic curves it is customary to use the notation $C_f = A[y]/\langle f(y)\rangle$. An alternative notation which is typically used in algebraic number theory is as follows: Assume f is irr. Fix an algebraic closure $\bar{K}$ of $K = \mathrm{Frac}\, A$ and let $\alpha \in \bar{K}$ be a root of $f(y)$. Then it is a standard fact that

$$A[y]/\langle f(y)\rangle \cong A[\alpha]$$

Indeed the ring hom $\varphi: A[y] \to A[\alpha]$ obtained by sending y to α is surjective with kernel $\langle f(y)\rangle$. Indeed, we are costumed to identify $\mathbb{C} = \mathbb{R}[i]$ with $\mathbb{R}[y]/\langle y^2+1\rangle$ where i corresponds to $y + \langle y^2+1\rangle$.

We'll use both notations, each when most convenient, and identify $C_f = A[y]/\langle f(y)\rangle$ with $A[\alpha]$.

Let $P \in \operatorname{Max} A$. To factor PC_f we'll first identify all maximal ideals in C_f that contain PC_f. We'll use the following notation: if $h(y) \in A[y]$ then we write $\bar{h}(y)$ for the reduction of $h(y)$ in $(A/P)[y]$.

First, factor $\bar{f}(y)$ into irr in $(A/P)[y]$ to obtain

$$\bar{f}(y) = \prod_{i=1}^{s} \bar{g}_i(y)^{e_i}$$

with $\bar{g}_i(y)$ monic and irr in $(A/P)[y]$. Let $g_i(y) \in A[y]$ be s.t. $\bar{g}_i(y)$ is the reduction of $g_i(y)$ in $(A/P)[y]$. Then $\exists h(y) \in PA[y]$ s.t.

$$f(y) = \prod_{i=1}^{s} g_i(y)^{e_i} + h(y).$$

Let $g_i(\alpha)$ be the image of $g_i(y)$ in $C_f \cong A[\alpha]$. Let $M_i = \langle P, g_i(\alpha) \rangle$ (in $C_f = A[\alpha]$).

Claim

M_i is maximal.

Proof

$$C_f/M_i \cong A[x]/\langle P, g_i(x)\rangle$$

$$\cong \left(A[y]/\langle f(y)\rangle\right)_{\langle P, g_i(y)\rangle}$$

$$\cong (A/P)[y]/\langle \bar{f}(y), \bar{g}_i(y)\rangle$$

$\bar{g}_i(y) \mid \bar{f}(y)$

$$= (A/P)[y]/\langle \bar{g}_i(y)\rangle$$

To conclude the proof we'll show that $(A/P)[y]/\langle \bar{g}_i(y)\rangle$ is a field, which will follow (in fact, is equivalent) to showing that $\langle \bar{g}_i(y)\rangle \in \mathrm{Max}\,(A/P)[y]$. Now, $P \in \mathrm{Max}\, A \Rightarrow A/P$ field $\Rightarrow (A/P)[y]$ PID and so $\bar{g}_i(y) \in \mathrm{Max}(A/P)[y]$ follows from the fact that $\bar{g}_i(y)$ is irr. ∎

The max ideals in C_f that contain PC_f are in 1:1 correspondence with the max ideals of C_f/PC_f. Now,

$$C_f/PC_f \cong (A[y]/\langle f(y)\rangle)/P$$

$$\cong (A/P)[y]/\langle \bar{f}(y)\rangle.$$

The only max ideal in $(A/P)[y]$ that contain $\langle \bar{f}(y)\rangle$ are $\langle \bar{g}_i(y)\rangle$ $i=1,\dots,s$ and so the max ideals of C_f containing PC_f are $M_1,\dots,M_s$.

Note further that since $C_f/M_i \cong (A/P)[y]/\langle \bar{g}_i(y)\rangle$ and since $\deg g_i(y) = \deg \bar{g}_i(y)$ we get that

$$[C_f/M_i : A/P] = \deg g_i(y)$$

Further,

$$[L:K] = \deg f = \sum_{i=1}^{s} e_i \cdot \deg g_i(y).$$

Proposition

Using the above notation, $PC_f \supseteq M_1^{e_1} \cdots M_s^{e_s}$. Equality holds when C_f is D.D, and $f_{M_i|P} = \deg g_i(y)$.

Proof

$$\prod_{i=1}^{s} M_i^{e_i} = \prod_{i=1}^{s} \langle P, g_i(\alpha) \rangle^{e_i}$$

$$\subseteq \langle P, \prod_{i=1}^{s} g_i(\alpha)^{e_i} \rangle$$

Recall that $h(y) \in PA[y]$ and so $h(\alpha) \in PC_f$. As $f(\alpha) = 0$ we get

$$\prod_{i=1}^{s} g_i(\alpha)^{e_i} \in \langle h(\alpha) \rangle \subseteq PC_f$$

$$\Rightarrow \prod_{i=1}^{s} M_i^{e_i} \subseteq PC_f.$$

Assume now that C_f is a D.D. In particular, C_f is integrally closed. Since f is monic, every element of C_f is integral over A. Thus, C_f is the integral closure of A in L.

Observe further that since f monic, C_f is a fg. A-module: $C_f = 1\cdot A + \alpha\cdot A + \cdots + \alpha^{n-1}A^{n-1}$. Thus, we may apply the fundamental equality and deduce $PC_f = \prod_{i=1}^{s} M_i^{e_{M_i|F}}$ and $[L:K] = \sum_{i=1}^{s} e_{M_i|P} f_{M_i|P}$. As

$$\Pi M_i^{e_i} \subseteq PC_f = \Pi M_i^{e_{M_i|P}}$$

we get $e_i \geq e_{M_i|P}$. Further, $f_{M_i|P} = \deg g_i(y)$ and so it must be that $e_i = e_{M_i|P}$.

∎