A direct proof of the Dedekind-Mertens Lemma

April 5, 2006

Let $P = f_0 + \ldots + f_n X^n$, $Q = g_0 + \ldots + g_m X^m$ and $R = PQ = h_0 + \ldots + h_{n+m} X^{n+m}$. *Dedekind-Mertens lemma* states that we have $c(P)^{m+1}c(Q) = c(P)^m c(R)$ where $c(S)$ denotes the *content* of a polynomial S, i.e. the ideal generated by the coefficients of S. We assume P, Q polynomials in $A[X]$ where A is an arbitrary commutative ring. In particular, A can be $\mathbb{Z}[f_0, \ldots, f_n, g_0, \ldots, g_m]$ where $f_0, \ldots, f_n, g_0, \ldots, g_m$ are indeterminates. Only the inclusion $c(P)^{m+1}c(Q) \subseteq c(P)^m c(R)$ is nontrivial. This is a beautiful generalisation of "Gauss's lemma" which states $c(P)c(Q) = c(R)$ in the case of integer coefficients. The general statement appears for instance in [4] with a proof attributed to Artin. Another proof using Gröbner bases can be found in [1]. The purpose of this note is to present a simple direct proof of the Dedekind-Mertens lemma, which follows actually the same structure as the proof of Gauss's lemma.

Let F (resp. G, resp. H) be the additive subgroup of A ($\mathbb{Z}$-module) generated by the set of coefficients of the polynomial P (resp. Q, resp. R). If X, Y are two additive subgroups of A, we write XY for the additive subgroup generated by all products uv, with $u \in X$, $v \in Y$.

Theorem 0.1 $F^{m+1}G \subseteq F^m H$

Proof. By induction on m, which is the formal degree of Q. This is clear if $m = 0$. We write $f_l = 0$ if $l < 0$ or $l > n$. We let G_m be the additive subgroup generated by the coefficients g_l for $l < m$. Since $\Sigma_{j<m} f_{k-j} g_j = h_k - f_{k-m} g_m$ is in $H + g_m F$ we have by induction on m

$$F^m G_m \subseteq F^{m-1}(H + g_m F) \subseteq F^{m-1}H + F^m g_m$$

and so, for all i

$$f_i F^m G_m \subseteq F^m H + F^m f_i g_m$$

Notice that $f_i g_m \in H + f_{i+1} G_m + \ldots + f_n G_m$. It follows that we have

$$f_i F^m G_m \subseteq F^m H + f_{i+1} F^m G_m + \ldots + f_n F^m G_m$$

and so $f_i F^m G_m \subseteq F^m H$ for $i = n, n-1, \ldots$ as desired. □

A direct application of this result is the celebrated "Dedekind's Prague theorem" [3], which states that each product $f_i g_j$ is integral over the coefficients of the product polynomial R. Another direct application is the equality $c(P)c(Q) = c(R)$ if A is a Prüfer domain, that is an integral domain such that all finitely generated non zero ideals of A are invertible.

Our argument is actually reminiscent of, but formally simpler than, Dedekind's original proof [2], who noticed that another generating system for the $\mathbb{Z}$-module F^{m+1} is given by the determinants

$$\begin{vmatrix} f_{i_0} & f_{i_0-1} & \cdots & f_{i_0-m} \\ f_{i_1} & f_{i_1-1} & \cdots & f_{i_1-m} \\ \cdots & \cdots & \cdots & \cdots \\ f_{i_m} & f_{i_m-1} & \cdots & f_{i_m-m} \end{vmatrix}$$

where $0 \leq i_0 < \ldots < i_m \leq n+m$. The inclusion $F^{m+1}G \subseteq F^m H$ follows easily from this remark.

Acknowledgement

Thanks to Harold Edwards for his comment on this note.

References

[1] Bruns, W. and Guerrieri, A. The Dedekind-Mertens formula and determinantal rings. Proc. Amer. Math. Soc. 127 (1999), no. 3, 657–663.

[2] Dedekind, R. Über einen arithmetischen Satz von Gauss. *Werke*, Vol.2, 28-38, 1892.

[3] Edwards, H. *Divisor Theory.* Birkhäuser Boston, Inc., Boston, MA, 1990.

[4] Northcott, D. G. A generalization of a theorem on the content of polynomials. Proc. Cambridge Philos. Soc. 55 1959 282–288.