Radical content

August 8, 2018

Let $\mathbf{R}$ be a commutative ring with 1. Let $f = a_0 + a_1X + \cdots + a_kX^k \in \mathbf{R}[X]$. The *radical content* $\mathsf{c}(f)$ of f is defined as the radical of the ideal generated by the coefficients of f, i.e.,

$$\mathsf{c}(f) = \sqrt{\langle a_0, \ldots, a_k \rangle}.$$

The following is a well-known generalization of Gauß' Lemma on primitive polynomials [4].

Proposition. *If $f = a_0 + a_1X + \cdots + a_kX^k$ and $g = b_0 + b_1X + \cdots + b_\ell X^\ell$, then*

$$\mathsf{c}(f) \cap \mathsf{c}(g) = \mathsf{c}(fg).$$

By passing to the quotient modulo a generic prime ideal, in classical mathematics this proposition reduces to the case of an integral ring [3]. Close inspection of the classical argument has led Banaschewski and Vermeulen to give two elementary constructive proofs [1], the second of which will here be recast in terms of the single-conclusion entailment relation of radical ideal [5]:

$$U \rhd a \;\equiv\; a \in \sqrt{\langle U \rangle}.$$

Recall that

$$\frac{U, a \rhd c \quad U, b \rhd c}{U, V, ab \rhd c} \tag{1}$$

Proof of the proposition. We closely follow [1]. Write

$$c_s = \sum_{\substack{i,j \\ i+j=s}} a_ib_j \quad (0 \leqslant s \leqslant k + \ell).$$

These are the coefficients of fg. The non-trivial inclusion is $\mathsf{c}(f) \cap \mathsf{c}(g) \subseteq \mathsf{c}(fg)$. Taking into account that

$$\mathsf{c}(f) \cap \mathsf{c}(g) \subseteq \sqrt{\langle a_0b_0, \ldots, a_ib_j, \ldots, a_kb_\ell \rangle},$$

due to transitivity it suffices to show that

$$c_0, c_1, \ldots, c_{k+\ell} \rhd a_ib_j \quad (0 \leqslant i \leqslant k, 0 \leqslant j \leqslant \ell),$$

to which end we argue by induction on $n = i + j$. The case $n = 0$ is obvious. Next suppose that the condition holds for all a_pb_q where $p + q < n$. Consider any i, j such that $i + j = n$. Then

$$a_ib_j = c_n - \sum_{\substack{p<i \text{ or } q<j \\ p+q=n}} a_pb_q.$$

This identity witnesses

$$c_n, \{\, a_pb_q : p < i \text{ or } q < j, p + q = n \,\} \rhd a_ib_j,$$

from which by monotonicity and transitivity with $a_p \rhd a_p b_q$ and $b_q \rhd a_p b_q$ we obtain

$$c_n, \{ a_p : p < i \}, \{ b_q : q < j \} \rhd a_i b_j.$$

Repeated application of (1) with $a_i \rhd a_i b_j$, resp. $b_j \rhd a_i b_j$, yields

$$c_n, \{ a_p b_j : p < i \}, \{ a_i b_q : q < j \} \rhd a_i b_j.$$

By way of the induction hypothesis, we know that

$$c_0, c_1, \ldots, c_{k+\ell} \rhd a_p b_j \quad (p < i) \qquad \text{and} \qquad c_0, c_1, \ldots, c_{k+\ell} \rhd a_i b_q \quad (q < j).$$

Therefore, repeated application of transitivity yields

$$c_0, c_1, \ldots, c_{k+\ell} \rhd a_i b_j. \qquad \square$$

Remark. The proposition is a consequence of the Dedekind-Mertens Lemma, a short constructive proof of which has been given by Coquand [2]

References

[1] B. Banaschewski and J.J.C Vermeulen. "Polynomials and radical ideals". In: *Journal of Pure and Applied Algebra* 113.3 (1996), pp. 219–227.

[2] Thierry Coquand. *A direct proof of the Dedekind-Mertens Lemma*. 2006. URL: `http://www.cse.chalmers.se/~coquand/mertens.pdf`.

[3] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Graduate Texts in Mathematics. Springer, 2004.

[4] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*. Dordrecht: Springer Netherlands, 2015.

[5] Davide Rinaldi, Peter Schuster, and Daniel Wessel. "Eliminating disjunctions by disjunction elimination". In: *Indagationes Mathematicae* 29.1 (2018), pp. 226–259.