

Loos, R.

Computing in algebraic extensions. (English) [Zbl 0576.12001](#)

Computer algebra, symbolic and algebraic computation, Comput. Suppl. 4, 173-187 (1982).

Summary: [For the entire collection see [Zbl 0491.00019](#).]

The aim of this chapter is an introduction to elementary algorithms in algebraic extensions, mainly over \mathbb{Q} and, to some extent, over $\text{GF}(p)$. We will talk about arithmetic in $\mathbb{Q}(\alpha)$ and $\text{GF}(p^n)$ in Section 1 and some polynomial algorithms with coefficients from these domains in Section 2. Then, we will consider the field K of all algebraic numbers over \mathbb{Q} and show constructively that K indeed is a field, that multiple extensions can be replaced by single ones and that K is algebraically closed, i.e. that zeros of algebraic number polynomials will be elements of K (Section 4-6).

For this purpose we develop a simple resultant calculus which reduces all operations on algebraic numbers to polynomial arithmetic on long integers together with some auxiliary arithmetic on rational intervals (Section 3). Finally, we present some auxiliary algebraic number algorithms used in other chapters of this volume (Section 7). This chapter does not include any special algorithms of algebraic number theory. For an introduction and survey with an extensive bibliography the reader is referred to *H. G. Zimmer* [Computational problems, methods and results in algebraic number theory (Lect. Notes Math. 262) (1972; [Zbl 0231.12001](#))].

MSC:

[12-04](#) Software, source code, etc. for problems pertaining to field theory

[68W99](#) Algorithms in computer science

Cited in **1** Review
Cited in **25** Documents

Keywords:

[algorithms in algebraic extensions](#); [zeros of algebraic number polynomials](#); [resultant calculus](#)