Hamburger Beiträge zur Mathematik

Nr. 712, November 2017

Remarks on the Polynomial Decomposition Law

by Ernst Kleinert

Remarks on the Polynomial Decomposition Law

Abstract: we first discuss in some detail the relation between the Polynomial Decomposition Law and the general principle for the extension of valuations; then we turn to the question of what happens if the crucial hypothesis for the former is not satisfied; we conclude with a few remarks on the problem of monogeneity.

1. Let K be an algebraic number field with discriminant d_K , O its ring of integers, α a generating integral element and f(x) its minimal polynomial (over the rational field). Denoting by d(f) the discriminant of f , we have an equation

$$d(f) = | O : \mathbb{Z}[\alpha]|^2 \; d_K \quad ,$$

and we abbreviate the index by $j(\alpha)$. Let p be a rational prime and assume

(*) p does not divide $j(\alpha)$.

Then the prime decomposition of p in O (more precisely, of the principal ideal pO), can be read off from the prime decomposition of f(x) mod p in the polynomial ring $\mathbb{Z}/p\mathbb{Z}[x]$: if f(x) mod p has prime factors $g_1, \ldots, g_r$ with multiplicities $e_1, \ldots, e_r$ and degrees deg $g_i = f_i$, then pO has prime divisors $P_1, \ldots, P_r$ with the same multiplicities (= ramification indices) and residue class degrees $f(P_i/p) = [O/P_i : \mathbb{Z}/p\mathbb{Z}] = f_i$. The standard proof even gives generators for the P_i ; since this is irrelevant for our present purpose, we can argue more simply: using the Chinese Remainder Theorem for the ring $\mathbb{Z}/p\mathbb{Z}[x]$ we see that the $\mathbb{Z}/p\mathbb{Z}$-algebra $\mathbb{Z}/p\mathbb{Z}[x] / (f \bmod p)$ has r simple factors $A_i = \mathbb{Z}/p\mathbb{Z}[x] / (g_i^{\,ei})$; the multiplicity e_i is the composition length of A_i as regular module and f_i is the $\mathbb{Z}/p\mathbb{Z}$-dimension of the field $A_i /\mathrm{rad}\, A_i = \mathbb{Z}/p\mathbb{Z}[x] / (g_i)$. An analogous analysis applies to the $\mathbb{Z}/p\mathbb{Z}$ – algebra O/pO, using the prime decomposition of pO . But it follows from (*) that

$$\mathbb{Z}/p\mathbb{Z}[x] / (f \bmod p) \;\simeq\; O/pO$$

(apply the invariant factor theorem to the lattices $\mathbb{Z}[x] / (f(x)) \simeq \mathbb{Z}[\alpha] \subseteq O$). Hence these algebras share the numerical invariants which we have exhibited above, and this proves the polynomial decomposition law (PDL).

2. The general principle for the extension of valuations is as follows (we give only a sketch, referring to [**L**], p.38 for proofs and more details) . Let k be a field with a place v ; denote by k_v the completion of k with respect to v. Let K = k(a) be a finite separable extension of k and f(x) the minimal polynomial of a over k . If w is any place of K extending v , then the completion K_w is a finite extension of k_v , obtained by adjoining a root of f(x) ; conversely every such extension contains K as a dense subfield and carries a unique extension w of v; thus we obtain an extension of v to K simply by restricting w to K. Further, two such extensions of v are

equivalent if and only if the corresponding field extensions are conjugate over K_v . In terms of f(x) this reads as follows: if

$$f(x) = h_1(x) \ldots h_r(x)$$

is the prime decomposition of f(x) over k_v , then the fields $K_i := k_v[x] / (h_i(x))$ are all the possible K_w ' s , of degree deg $h_i(x)$. This principle, which we may call the polynomial extension law for valuations (PEL), is purely algebraic and applies also to archimedean valuations. This latter case, however, is rather trivial, since by Ostrowski´s theorem the only case of a proper extension is the one in which k_v is the real and K_w the complex field. If we denote (in the nonarchimedean case) by e_i and f_i the ramification index and residue field degree of the extension K_i / k_v , then we have the „fundamental“ formulas

$$[K_i : k_v] = e_i f_i \text{ , whence } [K : k] = e_1 f_1 + \ldots + e_r f_r .$$

3. The relation between the nonarchimedean valuations of a number field K and the prime ideals of its integral domain O consists simply in the fact that every such valuation arises from a prime ideal P of O , in the following way: for any nonzero $a \in K$ denote by $\nu(P,a)$ the exponent of P in the prime ideal decomposition of the principal broken ideal aO ; then the function $a \to \nu(P,a)$ is an exponential valuation of K. Conversely, let R be any valuation ring of K, corresponding to a exponential valuation ν . We first claim that O is a subring of R : for any $a \in O$ we have an equation

$$a^n = r_{n-1} a^{n-1} + \ldots . r_1 a + r_0$$

with integral coefficients r_i . This implies

$$\nu(a^n) = n\nu(a) \geq \min (\nu(r_i) + \nu(a^i)) \geq \min (i \nu(a))$$

since clearly $\nu(r_i) \geq 0$; but then we must have $\nu(a) \geq 0$, whence $a \in R$. Now let M be the maximal ideal of R and put $P = O \cap M$, a nonzero prime ideal of O. For $a \in O$ we then have $\nu(P,a) > 0$ if and only if $\nu(a) > 0$. Since K is the quotient field of O , this equivalence carries over to $a \in K$. Thus the two valuations are equivalent. It should be noted that this relation between integrality and valuations holds much more generally: if the integral domain R is contained in the field K (not necessarily the quotient field of R), then the integral closure of R in K equals the intersection of all valuation rings in K which contain R ; see [**G**], p.4. In particular, the (prime ideal) divisors of the rational prime p correspond bijectively to the extensions of the p-adic valuation from $\mathbb{Q}$ to K.

4. The link between PDL and PEL is, not surprisingly, Hensel's lemma. Let us return to the notations of section 1, including the hypothesis (*). It also implies that

$$\mathbb{Z}_p \otimes O \simeq \mathbb{Z}_p[x] / (f(x))$$

is the maximal $\mathbb{Z}_p$ – order in the product of fields $\mathbb{Q}_p \otimes K = K_1 \times \ldots \times K_r$, in fact, (*) is equivalent to the maximality. This means that, if $f(x) = h_1(x) \ldots h_r(x)$ is the prime decomposition of f(x) over $\mathbb{Q}_p$ (of course the factors are already in $\mathbb{Z}_p[x]$), then

$$\mathbb{Z}_p[x] / (f(x)) \simeq \mathbb{Z}_p[x] / (h_1(x)) \times \ldots \times \mathbb{Z}_p[x] / (h_r(x)) ,$$

and $\mathbb{Z}_p[x] / (h_i(x))$ is the maximal order in K_i (namely, the integral closure of $\mathbb{Z}_p$). Now $h_i(x)$ mod p must be some power of an irreducible g_i since otherwise Hensel's lemma would give a factorization of h_i , which is impossible. Furthermore, these g_i must be pairwise different, since otherwise $\mathbb{Z}_p[x] / (h_i(x)h_j(x))$ mod p would contain no nontrivial idempotents, but of course it follows from the preceding isomorphism that

$$\mathbb{Z}_p[x] / (h_i(x)h_j(x)) \simeq \mathbb{Z}_p[x] / (h_i(x)) \times \mathbb{Z}_p[x] / (h_j(x))$$

is a direct sum, and the same holds mod p. Now it follows from PEL (plus the correspondence of section 3) that PDL gives the correct number of primes over p in K. It further follows from the maximality of $\mathbb{Z}_p[x] / (h_i(x))$ in K_i that deg g_i is the correct residue class degree of the extension $K_i / \mathbb{Q}_p$; and the local „fundamental“ formula finally ensures that the exponent of g_i in h_i mod p is the ramification index of this extension. Conversely, start with the prime decomposition

$$f \bmod p = g_1^{e1} \ldots\ldots g_r^{er}$$

and put $F_i = g_i^{ei}$; then by Hensel's lemma the decomposition f mod p $= F_1 \ldots F_r$ can be lifted to $\mathbb{Z}_p[x]$, with factors k_i mod $p = F_i$. The k_i must be irreducible, since from PDL (plus the correspondence) we know that the algebra $\mathbb{Q}_p \otimes K$ has exactly r primitive idempotents , but there would be more if a k_i were reducible. That the e_i and f_i (the global ramification indices and residue degrees) are the correct local quantities simply follows from the fact that these quantities do not change when passing to the completion.

5. The preceding discussion throws some light on what is going on if condition (*) does not hold. Write $\mathbb{Z}_p[x] / (h_i(x)) \simeq \mathbb{Z}_p(\alpha_i)$ for some zero α_i of h_i ; this is the image of $\mathbb{Z}_p[x] / (f(x))$ in the field K_i . The non-maximality of $\mathbb{Z}_p[x] / (f(x))$ in the algebra $K_1 \times \ldots \times K_r$ can have two sources: firstly, the $\mathbb{Z}_p(\alpha_i)$ need not be maximal; secondly, there may be bindings between the various $\mathbb{Z}_p(\alpha_i)$, in other words, $\mathbb{Z}_p[x] / (f(x))$ may not contain a full set of primitive idempotents of the algebra $K_1 \times \ldots \times K_r$. Of course the two possibilities can combine, and any non-maximal order must have at least one of these „defects“. Here are simple examples of these phenomena: let $f(x) = x^2 - 5$, p = 2; we have f(x) mod $2 = (x - 1)^2$, so from the PDL– formula we would get r = f = 1, e = 2; but here $\mathbb{Z}_2(\alpha)$ is not maximal; the maximal order is

generated by $(1+\alpha)/2$, which has minimal polynomial $x^2 - x - 1$, and the correct values are $f = 2$, $r = e = 1$. The second possibility is exemplified by Dedekind's example of an essential discriminant divisor; here $f(x) = x^3 + x^2 - 2x + 8$. The element $\beta = (\alpha + \alpha^2)/2$ has minimal polynomial $g(x) = x^3 - 2x^2 + 3x - 10$, hence is integral; f has discriminant -4×503, and it follows that α and β generate the maximal order, which has discriminant -503. Let $p = 2$. We have $f(x) \bmod 2 = x^2(x + 1)$, so by Hensel's lemma f(x) decomposes over $\mathbb{Z}_2$, $f(x) = k_1(x)k_2(x)$, with $k_2(x)$ corresponding to $x+1$, hence linear; we still must decide wether $k_1(x)$ is irreducible or split. Here we have an ad-hoc argument, knowing from the outset that 2 is unramified: if $k_1(x)$ were irreducible, then $\mathbb{Z}_2[x] / k_1(x)$ would be an order in the unramified quadratic extension of $\mathbb{Q}_2$, but an order mod 2 (in any unramified extension) could not contain nilpotents. Of course the splitting can be checked in other ways; by direct computation with the prime ideals (see e.g. [**C**], ex. 10.4, p.100) ; or noting that α has norm -8 and $\alpha+1$ has norm 10, and using the fundamental formula (taken from [**K**], p.94). Thus the PDL – formula gives $r = 2$, $e_1 = 2$, $e_2 = 1$ and all f's $= 1$; the correct values are $r = 3$, all e's and f's $= 1$. So $f(x)$ splits into linear factors, $f(x) = (x - a)(x - b)(x - c)$ over $\mathbb{Z}_2$ with $a \equiv b \equiv 0$, $c \equiv 1 \bmod 2$. In order to see the structure of our order, we lift the idempotents from $\mathbb{Z}_2[x] / (f(x),2)$ and obtain a decomposition $\mathbb{Z}_2[x] / (f(x)) = A \times \mathbb{Z}_2$ with some order $A \subseteq \mathbb{Z}_2 \times \mathbb{Z}_2$. One checks immediately that the map $x \to (a , b)$ induces an embedding

$$\mathbb{Z}_2[x] / (x - a)(x - b) \to A := \{(m,n) \mid m \equiv n \bmod 2\} ,$$

which must be surjective since both orders have index 2 in the maximal order (the surjectivity may also be checked directly by a somewhat tedious calculation with the coefficients of the polynomials involved). If one identifies $\mathbb{Q}_2[x] / (f(x)) = \mathbb{Q}_2{}^3$, then the order $\mathbb{Z}_2[x] / (f(x))$ contains only the idempotents (1,1,0) and (0,0,1). The primitive idempotent corresponding to the factor x^2 of $f(x) \bmod 2$ can be lifted to $\mathbb{Z}_2[x] / (f(x))$, but the lifted idempotent is no longer primitive in the surrounding algebra. (The lifting of idempotents from R-algebras $R[x] \bmod (f(x), P)$ to $R[x]/(f(x))$, where R is a complete discrete valuation ring with prime ideal P, may be viewed as a form of Hensel's lemma; see [**J**], II.3 for this connection.) In general the bindings between the orders $\mathbb{Z}_p(\alpha_i)$ can become arbitrarily complicated and need not consist in simple congruences among the factors. (Try describing $\mathbb{Z}_p[x]/(x^q - 1)$, where q is some power of p, as a suborder of the maximal order in the product of the corresponding cyclotomic fields.)

These examples indicate what happens in general. Let us first assume (as in the first example) that k_i (as above) is irreducible, but that $\mathbb{Z}_p(\alpha_i)$ is a proper suborder of O_i, the maximal order in K_i. Let P_i be the prime ideal of O_i and assume that this is unramified over $\mathbb{Z}_p$; then it follows from Nakayama's lemma that $\mathbb{Z}_p(\alpha_i) \bmod \mathbb{Z}_p(\alpha_i) \cap P_i$ must be a proper subfield of $O_i \bmod P_i$ (this is not in general true in the ramified case); but the degree of this subfield is $\deg g_i$ (in the previous notation). Thus the residue class degree comes out too small; but since the local fundamental

formula still holds, there must be a „pseudo“ ramification index to compensate for this. Going to the other extreme, let us assume that $k = k_1$ (say) is reducible, and that $k = h_1(x) \dots h_e(x)$ is its factorization into irreducibles, $e = e_1$, with all $h_i \bmod p = g_1$. Then the PDL – formula gives a single prime with residue class degree $\deg g_1$ and a pseudo ramification index e, whereas the correct ramification data consist in e primes, all having degree $\deg g_1$ and ramification index 1; this is what happens in the second example above. One sees in this way that, generally, the number of primes as well as the residue class degrees can come out too small, so that there must be pseudo ramification indices to compensate for this in the fundamental formula. Note however that, even if (*) is not satisfied, the decomposition data given by the PDL – formula may still be correct, an example of which is furnished by $f(x) = x^2 - 8$; but one sees from the preceding discussion that this can only happen if the primes dividing $j(\alpha)$ are ramified. Of course, the question arises whether one can define „optimal“ α's for which the deviation of the PDL – formula from the true decomposition data is minimal. The consequences of „unjudicious“ choices are illustrated already in our first example; more generally, note that for every integral α (of degree n) the minimal polynomial of pα is $\equiv x^n \bmod p$, so the PDL – formula does not tell us anything at all. Another natural strategy could be to combine informations coming from different α's.

6. At this point we have to adress here the question of essential discriminant divisors (paradoxically called „gemeinsame *außerwesentliche* Diskriminantenteiler“ in German, but both terminologies can be justified). If an integral generator α exists with $j(\alpha) = 1$, then O is said to possess a power integral basis, or to be monogeneous. The failure of this means that, for every α , there exists a prime dividing $j(\alpha)$. An „extreme“ case occurs when there is a single prime p dividing *all* $j(\alpha)$'s ; p is then called an essential discriminant divisor (EDD), and example 2 above is the simplest occurrence of this phenomenon. But already in pure cubic fields O may fail to be monogeneous; yet in these fields there are no EDD's; see [**C**], p.80 or [**H**], p.446ss for more details as well as some explicit examples. In these cases the equation $j(\alpha) = 1$ comes down to the solvability of certain diophantine equations. If no EDD's are present, one can obtain the full decomposition law by starting with any α and choosing for any prime divisor p of $j(\alpha)$ an integral β such that p does not divide $j(\beta)$. However, one cannot in this way arrive at a „good“ decomposition law, namely one of „class field type“; see for this my essay [**Kl**].

It is worth mentioning here that in extensions of p-adic fields the valuation ring of the extension field is always monogeneous over the one of the base field; see [**S**], prop.12, p.57. Viewed this way, the property of being non-monogeneous, like the property of not having unique prime factorization of elements, appears as a *purely* global phenomenon. However, from our present viewpoint it is not the monogeneity of the O_i which matters, but the maximality of the orders $\mathbb{Z}_p[x] / (f(x))$ in the algebras $\mathbb{Q}_p \otimes K = K_1 \times \dots \times K_r$ for all p, because for the maximality of orders a local-global-principle is valid (see [**R**], 11.2.). As we have pointed out earlier, our order will be maximal if and only if, for all p, (1) the number of prime divisors of p as

given by PDL is correct, and (2) $\mathbb{Z}_p(\alpha_i)$ equals the maximal order O_i of K_i, for all $i = 1,...,r = r_p$; a necessary, but not sufficient condition for the latter is that the corresponding residue class degree in the PDL-formula is correct. Here is an easy application: if a prime $p < n$ is completely split in K, then O cannot be monogeneous, because in the factorization of f(x) over $\mathbb{Z}_p$ some of the linear factors must be equal mod p, whence condition (1) is not satisfied. Of course this is well known since in this case p is even an EDD (see [**K**] l.c.).

Condition (1) may also be phrased as follows: let

$$f(x) = h_1(x) \dots h_r(x)$$

as before be the prime decomposition of f(x) over $\mathbb{Z}_p$; then (1) means that the prime ideals generated by the $h_i(x)$ are relatively prime *already over* $\mathbb{Z}_p$. Generally, let f(x), g(x) be two different (monic) irreducible polynomials over $\mathbb{Z}_p$; then we have an embedding of orders

$$\mathbb{Z}_p[x]/(f(x)g(x)) \to \mathbb{Z}_p[x]/(f(x)) \times \mathbb{Z}_p[x]/(g(x)), \quad F \bmod fg \to (F \bmod f, F \bmod g);$$

and if I denotes the ideal generated by f and g in $\mathbb{Z}_p[x]$, we can define a map (of additive groups)

$$\mathbb{Z}_p[x]/(f(x)) \times \mathbb{Z}_p[x]/(g(x)) \to \mathbb{Z}_p[x] / I, \quad (a \bmod f, b \bmod g) \to (a - b \bmod I),$$

and it is easy to show that the kernel of this map is exactly the image of the above embedding (one inclusion is obvious; for the other assume $a - b = cf - dg$ for some c,d in $\mathbb{Z}_p[x]$ and put $F = a - cf = b - dg$). Now $\mathbb{Z}_p \cap I = (p^s)$, some $s \geq 0$, because we have an equation $af + bg = 1$ with suitable a, b in $\mathbb{Q}_p[x]$; therefore (or by the above, because a suborder of an order always has finite index in the latter) $\mathbb{Z}_p[x] / I$ is a finite ring, whose cardinality equals the index of $\mathbb{Z}_p[x]/(f(x)g(x))$ in $\mathbb{Z}_p[x]/(f(x)) \times \mathbb{Z}_p[x]/(g(x))$. As seen earlier (by the lifting of idempotents), $s = 0$ if and only if f mod p and g mod p are relatively prime, whether or not f or g define maximal orders. On the other hand, if $s > 0$, then s (which may be viewed as sort of or part of a conductor) also reflects nonmaximality of the factors; for example if (f,g) = $(x^3 - p, x^4 - p)$, with both factors maximal, one obtains $s = 1$, but for the pair $(x^3 - p^2, x^4 - p^3)$, which defines nonmaximal orders in the same fields, one can show that $s = 4$. It may be worthwhile to explore in more detail the mechanics of such orders.

References

[**C**] H. Cohn, A Classical Invitation to Algebraic Numbers and Class Fields, Springer 1978;

[**G**] D. Goldschmidt, Algebraic Functions and Projective Curves, Springer GTM 2003;

[**H**] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin 1969;

[**J**] G. Janusz, Algebraic Number Fields, Academic Press 1973;

[**K**] H.Koch, Zahlentheorie, Braunschweig 1997;

[**Kl**] E.Kleinert, Über Zerlegungsgesetze, Hamburger Beiträge zur Mathematik 554 (2015);

[**L**] S. Lang, Algebraic Number Theory, Springer GTM 1986;

[**R**] I.Reiner, Maximal Orders, Academic Press 1975;

[**S**] J.-P. Serre, Local Fields, Springer GTM 1979.