

## ON $D_p$ -EXTENSIONS IN CHARACTERISTIC $p$

ARNE LEDET

(Communicated by Lance W. Small)

ABSTRACT. We study the relationship between generic polynomials and generic extensions over a finite ground field, using dihedral extensions as an example.

### 1. INTRODUCTION

Given a field  $K$  and a finite group  $G$ , we define a  $G$ -extension over  $K$  to be a Galois extension  $M/L$  with Galois group  $G$ , where  $L$  is a field containing  $K$ . When attempting to describe the “general form” of such an extension, the two principal structures are *generic polynomials* and *generic extensions*:

**Definition.** Let  $K$  be a field and  $G$  a finite group.

- (1) A *generic polynomial* for  $G$  over  $K$  is a monic polynomial  $P(\mathbf{t}, X) \in K(\mathbf{t})[X]$ , where  $\mathbf{t} = (t_1, \dots, t_n)$  are indeterminates, such that
  - (a) the Galois group of  $P(\mathbf{t}, X)$  over  $K(\mathbf{t})$  is  $G$ ; and
  - (b) when  $M/L$  is a  $G$ -extension over  $K$ , there exists  $\mathbf{a} = (a_1, \dots, a_n) \in L^n$  such that  $M$  is the splitting field over  $L$  of  $P(\mathbf{a}, X)$ .
- (2) A *generic extension* for  $G$  over  $K$  is a Galois extension  $S/R$  of commutative rings, with group  $G$ , such that
  - (a)  $R = K[\mathbf{t}, 1/u]$ , where  $\mathbf{t} = (t_1, \dots, t_n)$  are indeterminates and  $u \in K[\mathbf{t}] \setminus 0$ ; and
  - (b) when  $A/L$  is a Galois algebra with group  $G$  over a field  $L$  containing  $K$ , there exists a homomorphism  $\varphi: R \rightarrow L$  of  $K$ -algebras such that  $A/L \simeq S \otimes_R L/L$  (as Galois extensions).

The  $\mathbf{a}$  in (1)(b) and the  $\varphi$  in (2)(b) are both referred to as *specializations*, and the indeterminates  $\mathbf{t}$  are the *parameters*.

Generic extensions were introduced by Saltman in [Sa], whereas generic polynomials seems to be something of a “folklore” concept: In various forms, it is discussed in papers such as [Ku, 1964], [DM, 1983] and [Sm, 1991], and even as far back as [Noe, 1916]. Generic polynomials are sometimes required to be separable, but we will not impose this condition here, since it is not needed for our arguments.

It is hardly surprising that the concepts of generic polynomials and generic extensions are related. In fact, it is perfectly obvious that a generic extension gives rise to a generic polynomial: Any monic polynomial  $P(\mathbf{t}, X) \in R[X]$  whose roots generate  $S$  over  $R$  is generic.

---

Received by the editors April 23, 2003 and, in revised form, June 2, 2003.  
2000 *Mathematics Subject Classification.* Primary 12F12; Secondary 12E10, 13B05.

The relation the other way around was considered by Kemper in [Ke], where he proved that the existence of a generic polynomial over an *infinite* field  $K$  implies the existence of a generic extension. An outline of a proof (somewhat different from Kemper's, although fundamentally the same idea) is as follows: Let  $P(\mathbf{t}, X) \in K(\mathbf{t})[X]$  be a generic polynomial, and pick  $u \in K[\mathbf{t}]$  such that  $P(\mathbf{t}, X) \in K[\mathbf{t}, 1/u, X]$ . Let  $R = K[\mathbf{t}, 1/u]$ , and let  $S$  be the subring of the splitting field of  $P(\mathbf{t}, X)$  obtained by adjoining the roots of  $P(\mathbf{t}, X)$  to  $R$ . By choosing  $u$  properly, we can ensure that  $S/R$  is Galois with group  $G$ , and that it will be generic.

A consequence of this result is that, over an infinite field  $K$ , the existence of a generic extension and a generic polynomial are equivalent, and one can be constructed having the same set of parameters as the other.

Whether the existence of generic extensions and generic polynomials are equivalent over a *finite* field is not clear. Some results regarding the two concepts in that situation are given in [D&M]. It is known that both structures exist in a number of cases, such as  $p$ -groups in characteristic  $p$  (cf. [Le]).

The purpose of this paper is to prove the following result:

**Theorem.** *Let  $p$  be an odd prime, and let  $D_p$  denote the dihedral group of order  $2p$ . Then the following statements hold:*

- (i) *There is a 1-parameter generic polynomial for  $D_p$  over  $\mathbb{F}_p$ .*
- (ii) *There is a 2-parameter generic extension for  $D_p$  over  $\mathbb{F}_p$ .*
- (iii) *There is no 1-parameter generic extension for  $D_p$  over  $\mathbb{F}_p$ .*

In particular—and this is the point of the theorem—there can be no straightforward equivalence of generic extensions and generic polynomials over finite fields, the way there is over infinite fields.

## 2. PROOF OF THE THEOREM

In this section,  $p$  denotes an odd prime, and all fields are assumed to have characteristic  $p$ . The dihedral group  $D_p$  is represented as

$$D_p = \langle \sigma, \tau \mid \sigma^p = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle.$$

Also,  $C_n$  denotes the cyclic group of order  $n$ .

**Point (i).** It is proved in [Le] (and also in [JL&Y, Ch. 5]) that

$$X^p - 2X^{(p+1)/2} + X - t$$

is generic for the dihedral group  $D_p$  over any field of characteristic  $p$ , with  $t$  as the only parameter. (The idea of the proof is that a  $D_p$ -extension  $M/K$  in characteristic  $p$  always has the form  $M = K(\theta)$ , where  $\sigma\theta = \theta + 1$  and  $\tau\theta = -\theta$ ; cf. point (ii) below. The minimal polynomial for  $\theta^2$  over  $K$  is then as above.)

**Point (ii).** Let  $S = \mathbb{F}_p[s, t, 1/t]$ , and let  $D_p$  act on  $S$  by

$$\sigma: s \mapsto s + 1, \quad t \mapsto t$$

and

$$\tau: s \mapsto -s, \quad t \mapsto -t.$$

Then  $S/S^{D_p}$  is a Galois extension, since  $\sigma^i s - s = i \in S^*$  for  $p \nmid i$ , and  $\sigma^i \tau t - t = 2t \in S^*$  for all  $i$ . Also,  $R = S^{D_p} = \mathbb{F}_p[u, v, 1/v]$ , where  $u = (s^p - s)t$  and  $v = t^2$ .

We claim that  $S/R$  is a generic  $D_p$ -extension over  $\mathbb{F}_p$ .

Let  $K$  be a field (of characteristic  $p$ ), and let  $A/K$  be a Galois algebra with group  $D_p$ .

Since the additive first cohomology group is always trivial for Galois extensions of commutative rings, we in particular have  $H^1(C_p, A^+) = 0$ , and hence there exists an element  $\theta \in S$  with  $\sigma\theta = \theta + 1$ . From  $\sigma\tau\theta = \tau\sigma^{-1}\theta = \tau\theta - 1$ , we then conclude that  $\tau\theta = -\theta + x$  for an  $x \in A^{C_p}$ . Moreover,  $\theta = \tau^2\theta = \theta + \tau x - x$ , and so  $x \in K$ . Replacing  $\theta$  by  $\theta - \frac{1}{2}x$ , we get  $\sigma\theta = \theta + 1$  and  $\tau\theta = -\theta$ .

Next, consider the  $C_2$ -extension  $A^{C_p}/K$ . It is either a quadratic field extension, or the split extension  $K^2/K$  with  $C_2$  acting by  $\tau: (x, y) \mapsto (y, x)$ . In either case, we have  $\xi \in (A^{C_p})^*$  with  $\tau\xi = -\xi$ .

The specialization of  $S/R$  to  $A/K$  is now given by  $s \mapsto \theta$  and  $t \mapsto \xi$ .

**Point (iii).** We start by recalling the well-known fact that the automorphism group for a rational extension  $K(t)/K$  is the projective general linear group  $\text{PGL}_2(K)$ , with the automorphism corresponding to a matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  being given by

$$t \mapsto \frac{at + c}{bt + d}.$$

**Lemma.** *Let  $K$  be a field of characteristic  $p$ . Then  $D_p$  embeds into  $\text{PGL}_2(K)$  by*

$$\sigma \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and up to conjugation this is the only embedding.

*Proof.* First of all, it is trivial to check that this is an embedding. (In fact, it is also an embedding into the general linear group  $\text{GL}_2(K)$ .)

Next, let  $\sigma \mapsto \mathbf{A}$ ,  $\tau \mapsto \mathbf{B}$  be an embedding. Then  $\mathbf{A}^p = a\mathbf{E}$  for some  $a \in K^*$ , where  $\mathbf{E}$  is the  $2 \times 2$  identity matrix. Thus,  $\mathbf{A}$  is a root of  $X^p - a$ , as well as of  $X^2 - \text{Tr } \mathbf{A} \cdot X + \det \mathbf{A}$ . Since  $\mathbf{A}$  is not a scalar matrix, the greatest common divisor of these two polynomials cannot have degree 1, and therefore it must be  $X^2 - \text{Tr } \mathbf{A} \cdot X + \det \mathbf{A}$ . Hence,  $X^2 - \text{Tr } \mathbf{A} \cdot X + \det \mathbf{A} = (X - \sqrt[p]{a})^2$ , and  $a$  is a  $p$ th power in  $K$ . Scaling  $\mathbf{A}$  by  $1/\sqrt[p]{a}$ , we get  $\mathbf{A}^p = \mathbf{E}$ .

Since the characteristic polynomial for  $\mathbf{A}$  is  $(X - 1)^2$ , it has 1 as its only eigenvalue, and is therefore conjugate to a matrix of the form  $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ ,  $x \neq 0$ . From

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

we then get that  $\mathbf{A}$  is conjugate to  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ , and that we may assume  $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .

Now,  $\mathbf{B}\mathbf{A}\mathbf{B}^{-1} = y\mathbf{A}^{-1}$  for a  $y \in K^*$ , and taking determinants gives us  $y^2 = 1$ , i.e.,  $y = \pm 1$ . A simple calculation shows that  $y = 1$  and  $\mathbf{B} = \begin{pmatrix} s & 0 \\ t & -s \end{pmatrix}$ . Scaling  $\mathbf{B}$  by  $1/s$  allows us to replace  $\mathbf{B}$  by  $\begin{pmatrix} 1 & 0 \\ t & -1 \end{pmatrix}$ , and since

$$\begin{pmatrix} 1 & 0 \\ -1-t & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1-t & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ -1-t & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1-t & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

we have the result. □

In terms of the automorphism group, this means that  $D_p$  acts on  $K(t)$  by

$$\sigma: t \mapsto t + 1, \quad \tau: t \mapsto -t,$$

and any faithful  $D_p$ -action on  $K(t)$  is of this form, given a proper choice of the rational generator  $t$ .

Now, assume that  $S/R$  is a 1-parameter generic extension for  $D_p$  over  $\mathbb{F}_p$ . Since  $D_p$  acts on  $\mathbb{F}_p(t)$ , we have a  $D_p$ -extension  $\mathbb{F}_p(t)/\mathbb{F}_p(t)^{D_p}$ , and this is of course obtained by specializing  $S/R$ : For some  $\mathbb{F}_p$ -algebra homomorphism  $\varphi: R \rightarrow \mathbb{F}_p(t)^{D_p}$ , we have  $\mathbb{F}_p(t) \simeq S \otimes_{\varphi} \mathbb{F}_p(t)^{D_p}$ .

Of necessity,  $\varphi$  must be injective, meaning that we have  $R \hookrightarrow \mathbb{F}_p(t)^{D_p}$  and  $S \hookrightarrow \mathbb{F}_p(t)$ . The quotient fields  $Q(R)$  and  $Q(S)$  of  $R$  and  $S$ , resp., are therefore subfields of  $\mathbb{F}_p(t)$ , and so rational by Lüroth's Theorem. By the Lemma, the action of  $D_p$  on  $Q(S)$  is given, meaning that we may assume  $Q(S) = \mathbb{F}_p(t)$ .

It follows that  $Q(R) = \mathbb{F}_p(t)^{D_p} = \mathbb{F}_p(s)$ , where  $s = (t^p - t)^2$  (since  $s \in \mathbb{F}_p(t)^{D_p}$  and  $[\mathbb{F}_p(t) : \mathbb{F}_p(s)] = 2p$ ).

If  $R = \mathbb{F}_p[u, 1/v]$  ( $v \in \mathbb{F}_p[u]$ ), then  $u$  must be a rational generator for  $\mathbb{F}_p(s)/\mathbb{F}_p$ , i.e., of the form  $(as + b)/(cs + d)$  for  $a, b, c, d \in \mathbb{F}_p$ . Hence, either  $s \in R$ , or  $1/(s + i) \in R$  for an  $i \in \mathbb{F}_p$ .

Note that  $S$  is the integral closure of  $R$  in  $\mathbb{F}_p(t)$ .

If  $s \in R$ , then  $t \in S$  (since  $t$  is integral over  $\mathbb{F}_p[s]$ ). It follows that  $S$  is a localization of  $\mathbb{F}_p[t]$ :  $S = \mathbb{F}_p[t]_T$ , where  $T = \mathbb{F}_p[t] \cap R^*$ . Since  $\tau t - t = 2t$ , we have  $(\tau - 1)S \subseteq tS$ , and since  $S/R$  is Galois, we must therefore have  $t \in S^*$ . But then  $s \in R^*$ , since  $s$  is minus the norm of  $t$ .

Next, assume  $1/(s + i) \in R$  for some  $i \in \mathbb{F}_p$ . Then  $t/(s + i) \in S$ , since  $t/(s + i)$  is a root of

$$\left(X^p - \frac{1}{(s + i)^{p-1}}X\right)^2 + \frac{i}{(s + i)^{2p}} - \frac{1}{(s + i)^{2p-1}}.$$

**Lemma.** *Let  $U$  be a unique factorization domain with  $2 \in U^*$ . If  $a \in U \setminus U^2$  is square-free, then  $U[\sqrt{a}]$  is integrally closed.*

*Proof.*  $b + c\sqrt{a}$  is a root of  $X^2 - 2bX + (b^2 - ac^2)$ . The result follows easily.  $\square$

Let  $u = 1/(s + i)$ . Then  $u(1 - iu) = s/(s + i)^2$ , meaning that  $u(1 - iu)$  is a square in  $\mathbb{F}_p(t)$ , with square root  $(t^p - t)/(s + i)$ . Thus, the integral closure of  $R$  in  $\mathbb{F}_p(t)^{C_p} = \mathbb{F}_p(t^p - t)$  is  $R[\sqrt{u(1 - iu)}]$ . This must therefore be  $S^{C_p}$ , and so  $R[\sqrt{u(1 - iu)}]/R$  is a Galois extension with Galois group  $C_2$ , generated by  $\tau$ .

Since  $\tau(p + q\sqrt{u(1 - iu)}) - (p + q\sqrt{u(1 - iu)}) = 2q\sqrt{u(1 - iu)}$  for  $p, q \in R$ , we see that

$$(\tau - 1)R[\sqrt{u(1 - iu)}] \subseteq \sqrt{u(1 - iu)}R[\sqrt{u(1 - iu)}].$$

It follows that  $\sqrt{u(1 - iu)}$  is a unit in  $R[\sqrt{u(1 - iu)}]$ , and hence that  $u \in R^*$ , i.e.,  $s + i \in R$ , and so  $s \in R$ . As above, this means that  $s \in R^*$ .

But consider the split  $D_p$ -extension  $\mathbb{F}_p^{2p}/\mathbb{F}_p$ . It is also a specialization of  $S/R$ , and no matter what  $t$  is specialized to, the specialization of  $s = (t^p - t)^2$  will be 0, and not a unit.

This contradiction shows that there can be no one-parameter generic extension.

## REFERENCES

- [DM] F. R. DeMeyer, *Generic polynomials*, J. Algebra **84** (1983), 441–448. MR **85a**:12007
- [D&M] F. DeMeyer and T. McKenzie, *On generic polynomials*, J. Algebra **261** (2003), 327–333. MR **2003m**:12007
- [JL&Y] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Series 45, Cambridge University Press, Cambridge, 2002. MR **2004d**:12007
- [Ke] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141. MR **2002k**:12009
- [Ku] W. Kuyk, *On a theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A **67** = Indag. Math. **26** (1964), 32–39. MR **28**:3989
- [Le] A. Ledet, *On  $p$ -groups in characteristic  $p$* , in Algebra, Arithmetic and Geometry with Applications (Christensen, Sundaram, Sathaye, and Bajaj, eds.), Springer-Verlag, 2004, pp. 591–600.
- [Noe] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1916), 221–229.
- [Sa] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283. MR **84a**:13007
- [Sm] G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Algebra **19**(12) (1991), 3367–3391. MR **93d**:12004

DEPARTMENT OF MATHEMATICS AND STATISTICS, TEXAS TECH UNIVERSITY, LUBBOCK, TEXAS  
79409–1042

*E-mail address:* `aledet@math.ttu.edu`