

Diploma Thesis

On Theorems of Schur and Coleman in Galois Theory

English translation prepared from the German original

Orges Leka

27 May 2010

Supervisor: Prof. Dr. M. Lehn
Department 08 – Physics, Mathematics and Computer Science
Johannes Gutenberg University Mainz

Contents

Introduction	2
1 Auxiliary Results from Algebraic Number Theory	4
1.1 Newton Polygons	4
1.2 Different, Discriminant, and Dedekind	7
2 Auxiliary Results from Analytic Number Theory	9
2.1 The Theorem of Tschebyscheff–Bertrand	9
2.2 A Theorem of Schur–Sylvester	11
3 Auxiliary Results from Group Theory	16
3.1 Wreath Products and Imprimitve Groups	16
3.2 Transitive Groups	17
4 The Galois Group of $E_n(x)$ According to Schur	19
4.1 General Theorems for Computing Galois Groups	19
4.2 Concrete Calculations for $E_n(x)$	20
5 The Galois Group of $E_n(x)$ According to Coleman	23
6 Observations on $C_n(x)$	26
Bibliography	34
Acknowledgements	37
Declaration	38

Introduction

In this thesis we present two essentially different ways of proving the following theorem of Schur:

The Galois group over \mathbb{Q} of the exponential Taylor polynomial

$$E_n(x) = \sum_{k=0}^n \frac{x^k}{k!}$$

is the symmetric group S_n if $n \not\equiv 0 \pmod{4}$, and the alternating group A_n otherwise.

The original motivation for this work was to compute the Galois groups of the Taylor polynomial

$$C_n(x) = \sum_{k=0}^n \frac{x^{2k}}{(2k)!}.$$

For small values of n one is led to conjecture that the Galois group of $C_n(x)$ over \mathbb{Q} is the wreath product $S_2 \wr S_n$. The hope that one might prove this was inspired by the theorem of Schur just mentioned. Schur's proof uses results from analytic number theory—for instance the theorem of Schur–Sylvester on divisibility properties of consecutive integers by suitable primes—as well as results of Dedekind from algebraic number theory. This makes access to the Galois-theoretic statement somewhat difficult if one is interested mainly in the Galois group itself.

A different proof of Schur's theorem on the Galois group of $E_n(x)$ was found by Coleman. He uses Newton polygons and reaches the desired conclusion rather quickly. In this way he avoids both the Schur–Sylvester theorem from analytic number theory and the algebraic-number-theoretic results used by Schur. Both approaches, however, have in common that they use the theorem of Tschebyscheff–Bertrand (for $n \geq 8$ there is always a prime p with $n/2 < p < n - 2$) and a theorem of Jordan from group theory. Jordan's theorem gives practical criteria for deciding when a group G is the full symmetric group S_n or the alternating group A_n .

Unfortunately, within the scope of this thesis it was not possible to prove that the Galois group of $C_n(x)$ over \mathbb{Q} is $S_2 \wr S_n$. In trying to establish this conjecture one encounters, among other things, the difficulty of deciding when a subgroup $G \leq S_2 \wr S_n$ is in fact the whole wreath product. The author does not know an analogue for $S_2 \wr S_n$ of Jordan's theorem for S_n . We

can, however, show by the methods of Schur and Coleman that the Galois group of

$$\sum_{k=0}^n \frac{x^k}{(2k)!}$$

over \mathbb{Q} is either the alternating or the symmetric group.

Chapter 1

Auxiliary Results from Algebraic Number Theory

1.1 Newton Polygons

We begin with the definition and some basic properties of Newton polygons. See, for example, Neukirch, *Algebraic Number Theory*, or Gouvêa, *p-adic Numbers*.

Definition 1.1 (Newton polygon). *Let v be any exponential valuation on a field K , and let*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x], \quad a_0a_n \neq 0.$$

To each term a_ix^i we associate the point $(i, v(a_i)) \in \mathbb{R}^2$, ignoring (i, ∞) if $a_i = 0$. The lower convex hull of the set

$$\{(0, v(a_0)), (1, v(a_1)), \dots, (n, v(a_n))\}$$

is a polygonal path called the Newton polygon of $f(x)$.

For example, the Newton polygon of $f(x) = 6 + 9x + 10x^3 + 12x^4$ with respect to v_2 is given in Figure 1.1. With respect to v_3 one obtains the Newton polygon shown in Figure 1.2.

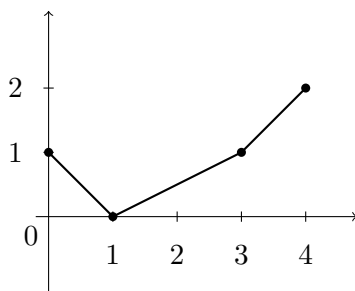


Figure 1.1: Newton polygon of $f(x) = 6 + 9x + 10x^3 + 12x^4$ with respect to 2.

As these examples show, the Newton polygon consists of line segments whose slopes increase strictly from left to right. The following theorem is standard.

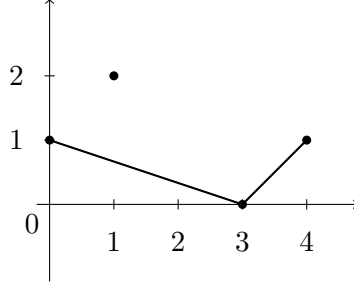


Figure 1.2: Newton polygon of $f(x) = 6 + 9x + 10x^3 + 12x^4$ with respect to 3.

Theorem 1.2 (Lengths of the line segments in the Newton polygon). *Let*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_0a_n \neq 0,$$

be a polynomial over a field K , let v be an exponential valuation on K , and let w be an extension of v to the splitting field L of f . Suppose that the segment joining $(r, v(a_r))$ and $(s, v(a_s))$ occurs in the Newton polygon and has slope $-m$. Then $f(x)$ has exactly $s - r$ zeros $\alpha_1, \dots, \alpha_{s-r}$ with

$$w(\alpha_1) = \cdots = w(\alpha_{s-r}) = m.$$

Proof. A proof may be found in Neukirch, pp. 145–146. Dividing by a_n merely shifts the polygon vertically, so we may assume $a_n = 1$. Number the roots $\alpha_1, \dots, \alpha_n \in L$ in such a way that

$$\begin{aligned} w(\alpha_1) &= \cdots = w(\alpha_{s_1}) = m_1, \\ w(\alpha_{s_1+1}) &= \cdots = w(\alpha_{s_2}) = m_2, \\ &\vdots \\ w(\alpha_{s_t+1}) &= \cdots = w(\alpha_n) = m_{t+1}, \end{aligned}$$

with $m_1 < m_2 < \cdots < m_{t+1}$. Viewing the coefficients a_i as elementary symmetric functions in the roots yields

$$\begin{aligned} v(a_n) &= v(1) = 0, \\ v(a_{n-1}) &\geq \min_j w(\alpha_j) = m_1, \\ v(a_{n-2}) &\geq \min_{i,j} w(\alpha_i\alpha_j) = 2m_1, \\ &\vdots \\ v(a_{n-s_1}) &\geq \min_{i_1, \dots, i_{s_1}} w(\alpha_{i_1} \cdots \alpha_{i_{s_1}}) = s_1m_1, \end{aligned}$$

and similarly for the remaining groups. Hence the vertices of the Newton polygon, read from right to left, are

$$(n, 0), (n - s_1, s_1m_1), (n - s_2, s_1m_1 + (s_2 - s_1)m_2), \dots$$

Therefore the slope of the rightmost edge is $-m_1$, and in general the next edge has slope $-m_{j+1}$. This proves the claim. \square

Lemma 1.3. *Keep the notation of the previous theorem. If the valuation v has a unique extension w to the splitting field L of f , then*

$$f(x) = \prod_{j=1}^r f_j(x)$$

is a factorization over K , where

$$f_j(x) = \prod_{w(\alpha_i)=m_j} (x - \alpha_i) \in K[x].$$

Proof. We may assume that $a_n = 1$. First suppose that $f(x)$ is irreducible. Then, by the transitivity of the Galois group $\text{Gal}(L/K)$ on the roots of f , we may write $\alpha_i = \sigma_i(\alpha)$ for suitable $\sigma_i \in \text{Gal}(L/K)$. Since for every extension w of v the composition $w \circ \sigma_i$ is again an extension of v , the uniqueness of the extension implies

$$w(\alpha_i) = w(\sigma_i(\alpha)) = w(\alpha).$$

Thus all roots of f have the same valuation, so in this case $f_1(x) = f(x)$ and the assertion follows.

For the general case we argue by induction on $n = \deg f$. There is nothing to prove for $n = 1$. Let $p(x)$ be the minimal polynomial of α_1 over K , and put

$$g(x) = \frac{f(x)}{p(x)} \in K[x].$$

Since all roots of $p(x)$ have the same valuation m_1 , the polynomial $p(x)$ divides $f_1(x)$. Let

$$g_1(x) = \frac{f_1(x)}{p(x)}.$$

By the previous theorem, the factorization of $g(x)$ is then given by

$$g(x) = g_1(x) \cdot \prod_{j=2}^r f_j(x).$$

Because $\deg g < \deg f$, the induction hypothesis applies to $g(x)$ and shows that $g_1(x), f_2(x), \dots, f_r(x)$ all lie in $K[x]$. Since also $p(x) \in K[x]$, it follows that

$$f_1(x) = p(x)g_1(x) \in K[x],$$

and therefore $f_j(x) \in K[x]$ for all $j = 1, \dots, r$. \square

Lemma 1.4. *Let $f(x)$ be a separable polynomial in $k[x]$, let K be its splitting field, and let*

$G = \text{Gal}(K/k)$. If

$$f(x) = f_1(x) \cdots f_r(x)$$

is the factorization into irreducibles over k and $n_i = \deg f_i$, then each n_i divides $|G|$.

Proof. Let Ω be the set of roots of f and Ω_i the set of roots of f_i . Then $K_i := k(\Omega_i)$ is an intermediate field of K/k . Since $n_i = \deg f_i$ divides $[K_i : k]$ and

$$[K : K_i][K_i : k] = [K : k] = |\text{Gal}(K/k)|,$$

it follows that $n_i \mid |G|$. □

Theorem 1.5 (Main theorem on Newton polygons). *Let p be a prime and let $f(x) \in \mathbb{Q}_p[x]$ have vertices $(x_0, y_0), (x_1, y_1), \dots, (x_r, y_r)$ in its Newton polygon. Then over \mathbb{Q}_p one has a factorization*

$$f(x) = f_1(x) \cdots f_r(x),$$

where $\deg f_j = x_j - x_{j-1}$ and every zero of f_j in $\overline{\mathbb{Q}_p}$ has valuation

$$-\frac{y_j - y_{j-1}}{x_j - x_{j-1}}.$$

If f is separable over \mathbb{Q}_p , then the order of its Galois group over \mathbb{Q}_p is divisible by $x_j - x_{j-1}$ for every j .

Proof. The first statement is the preceding lemma applied to the valuation classes determined by the Newton polygon. The second follows from the divisibility lemma for irreducible factors. □

1.2 Different, Discriminant, and Dedekind

Lemma 1.6 (Transitivity of the different and discriminant). *Let $K \subset K' \subset L$ be finite extensions of number fields. Then for the differentials and discriminants one has*

$$\mathfrak{D}_{L/K} = \mathfrak{D}_{K'/K} \mathfrak{D}_{L/K'}$$

and

$$D_{L/K} = D_{K'/K}^{[L:K']} N_{K'/K}(D_{L/K'}).$$

Theorem 1.7 (Dedekind's different theorem). *Let K'/K be an extension of number fields with relative different $\mathfrak{D}_{K'/K}$ and rings of integers $\mathcal{O}_{K'}$ and \mathcal{O}_K . Let $\mathfrak{P}' \neq 0$ be a prime ideal of $\mathcal{O}_{K'}$, with corresponding prime $\mathfrak{P} = \mathfrak{P}' \cap \mathcal{O}_K$ and ramification index $e = e(\mathfrak{P}'/\mathfrak{P})$. Then*

$$v_{\mathfrak{P}'}(\mathfrak{D}_{K'/K}) = e - 1 \quad \text{if } e \not\equiv 0 \pmod{p},$$

and

$$v_{\mathfrak{P}'}(\mathfrak{D}_{K'/K}) \geq e \quad \text{if } e \equiv 0 \pmod{p},$$

where p is the rational prime contained in \mathfrak{P} .

Proof. Let L/K be a Galois extension containing K' as an intermediate field, and let \mathfrak{P} be a prime of \mathcal{O}_L above the given prime. Writing $G = \text{Gal}(L/K)$ and $G' = \text{Gal}(L/K')$, and using the Hilbert ramification groups G_n and G'_n , one has $G'_n = G_n \cap G'$. Hilbert's formula gives

$$v_{\mathfrak{P}}(\mathfrak{D}_{L/K}) = \sum_{n \geq 0} (|G_n| - 1), \quad v_{\mathfrak{P}}(\mathfrak{D}_{L/K'}) = \sum_{n \geq 0} (|G'_n| - 1).$$

By transitivity of the different,

$$v_{\mathfrak{P}}(\mathfrak{D}_{K'/K}) = \sum_{n \geq 0} (|G_n| - |G'_n|).$$

Dividing by the residual ramification factor shows first that $v_{\mathfrak{P}}(\mathfrak{D}_{K'/K}) \geq e - 1$. If $e \not\equiv 0 \pmod{p}$, then the first higher ramification groups coincide, hence $G_n = G'_n$ for all $n \geq 1$, and equality $e - 1$ follows. If $e \equiv 0 \pmod{p}$, then the first higher ramification groups differ, so the valuation is strictly larger than $e - 1$, hence at least e . \square

Theorem 1.8 (Dedekind's criterion). *Let*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$$

be irreducible over \mathbb{Q} , with discriminant Δ . Let D be the discriminant of $\mathbb{Q}(\alpha)$ for a root α of f . Let p be a prime, and suppose that modulo p one has

$$\bar{f}(x) \equiv \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r},$$

with the f_i monic and irreducible modulo p . Define $m(x)$ by

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} - p m(x).$$

Then the following are equivalent:

1. $v_p(\Delta) > v_p(D)$;
2. *there exists some s such that $e_s > 1$ and $m(x) \equiv 0 \pmod{(p, f_s(x))}$ in $\mathbb{F}_p[x]/(f_s(x))$.*

Proof. For a proof of a version of this theorem, see for example Peter Schmid, *Algebraische Zahlentheorie*, lecture notes from the Winter Semester 2008/2009 (version of September 2008), Chapter 9 (*Ramification and Discriminant*), appendix (*Dedekind criterion*), p. 44. \square

Chapter 2

Auxiliary Results from Analytic Number Theory

In this chapter we prove, with the aid of several results of Tschebyscheff, the statements Schur uses to show that

$$E_n(x) = \sum_{k=0}^n \frac{x^k}{k!}$$

is irreducible over $\mathbb{Q}[x]$. We also derive the theorem of Tschebyscheff–Bertrand, since it is used in both Schur’s and Coleman’s approaches.

As usual, let $\pi(x)$ denote the number of primes $p \leq x$, and define

$$\vartheta(x) = \sum_{\substack{p \leq x \\ p \text{ prime}}} \log p.$$

Further, let

$$\Psi(x) = \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \dots = \sum_{m \geq 1} \vartheta(x^{1/m}).$$

Equivalently, $\Psi(x) = \sum_{p^m \leq x} \log p$.

2.1 The Theorem of Tschebyscheff–Bertrand

Theorem 2.1 (Tschebyscheff’s estimates for Ψ and ϑ). *Let*

$$a = \log(2^{1/2}3^{1/3}5^{1/5}30^{1/30}) = 0.92129\dots$$

Then:

$$\begin{aligned} \vartheta(x) &< \frac{6}{5}ax + 3 \log(x)^2 + 8 \log x + 5, \\ \vartheta(x) &> ax - \frac{12}{5}a\sqrt{x} - \frac{3}{2} \log(x)^2 - 13 \log x - 15, \\ \Psi(x) - \Psi(x^{1/6}) &< ax + 5 \log x + 5. \end{aligned}$$

Proof. Statements (i) and (ii) are classical results of Tschebyscheff; (iii) is also standard and may be found in Landau's *Handbuch der Lehre von der Verteilung der Primzahlen*. \square

Theorem 2.2 (An estimate for $\pi(x)$). *For $x \geq 2$ one has*

$$\pi(x) < \frac{3}{2} \cdot \frac{x}{\log x}.$$

Proof. It suffices to prove the inequality for integer x . For $x \leq 6^5 = 7776$ it can be checked directly with a computer algebra system. Assume now that $x > 6^5$. Then

$$\pi(x) - \pi(x/6) = \sum_{x/6 < p \leq x} \frac{\log p}{\log p} \leq \frac{\vartheta(x) - \vartheta(x/6)}{\log(x/6)} \leq \frac{\Psi(x) - \Psi(x^{1/6})}{\log(x/6)}.$$

Using the previous theorem,

$$\pi(x) - \pi(x/6) < \frac{ax + 5 \log x + 5}{\log(x/6)}.$$

By induction we may assume

$$\pi(x/6) < \frac{3}{2} \cdot \frac{x/6}{\log(x/6)}.$$

Adding these bounds gives

$$\pi(x) < \frac{1}{\log x - \log 6} (1.18x + 5 \log x + 5),$$

and one checks that this is $< \frac{3}{2} \frac{x}{\log x}$ for $x \geq 6^5$. \square

For the range $2 \leq x \leq 6^5 = 7776$, the original thesis records the following GP-PARI check:
`for(x=2,6^5,if(primepi(x)<3/2*x/log(x), , print("Inequality fails for:", x)))`

Theorem 2.3. *For $x \geq 29$ there is a prime p with*

$$x < p \leq \frac{5x}{4}.$$

Proof. Using the previous estimates for $\vartheta(x)$, one obtains for large x that

$$\vartheta(5x/4) - \vartheta(x) > \frac{1}{20}g(x),$$

where

$$g(x) = ax - 56a\sqrt{x} - 140 \log(x)^2 - 30 \log x - 4.$$

Since $g(x)$ is eventually positive and increasing, it suffices to check positivity at a suitable point; $x = e^{12}$ works. The remaining values $29 \leq x \leq e^{12}$ can be verified computationally. \square

For the finite range $29 \leq x \leq e^{12}$, the original thesis checks the claim in GP-PARI as follows:

`for(x=29, floor(exp(12)), if(primepi(5.0/4.0*x)>primepi(x), , print("No prime found for:",`

Theorem 2.4 (Tschebyscheff–Bertrand). *For every $n \geq 8$ there exists a prime p with*

$$\frac{n}{2} < p < n - 2.$$

Proof. Set $x = n/2$. For $n \geq 58$ we have $x \geq 29$, so by the previous theorem there exists a prime p with

$$\frac{n}{2} = x < p \leq \frac{5x}{4} = \frac{5n}{8} < n - 2.$$

The remaining values $8 \leq n < 58$ can be checked directly. \square

Lemma 2.5. *If a, b, c are positive integers, then*

$$\left\lfloor \frac{a+b}{c} \right\rfloor - \left\lfloor \frac{a}{c} \right\rfloor - \left\lfloor \frac{b}{c} \right\rfloor \in \{0, 1\}.$$

Proof. Write $a = qc + r_1$, $b = rc + r_2$ with $0 \leq r_1, r_2 < c$. Then either $r_1 + r_2 < c$, in which case the difference is 0, or $c \leq r_1 + r_2 < 2c$, in which case it is 1. \square

2.2 A Theorem of Schur–Sylvester

Theorem 2.6 (An inequality of Schur). *Let h, k be natural numbers such that the k consecutive integers*

$$h + 1, h + 2, \dots, h + k$$

are divisible only by primes $p \leq k$. Then

$$(h + k + \frac{1}{2} - \pi(k)) \log(h + k) < \frac{7}{6} + (h + \frac{1}{2}) \log h + (k + \frac{1}{2}) \log k.$$

Proof. By assumption the binomial coefficient $\binom{h+k}{k}$ is divisible only by primes $p \leq k$. Writing

$$\binom{h+k}{k} = \prod_{p \leq k} p^{\mu_p},$$

where

$$\mu_p = \sum_{\lambda} \left(\left\lfloor \frac{h+k}{p^\lambda} \right\rfloor - \left\lfloor \frac{h}{p^\lambda} \right\rfloor - \left\lfloor \frac{k}{p^\lambda} \right\rfloor \right),$$

the previous lemma shows that each summand is 0 or 1, hence

$$\mu_p \leq \frac{\log(h+k)}{\log p}.$$

If $T(n) = \log(n!)$, then

$$\Delta := T(h+k) - T(h) - T(k) = \log \binom{h+k}{k} \leq \pi(k) \log(h+k).$$

Applying Stirling's formula

$$T(n) = (n + \frac{1}{2}) \log n - n + \log \sqrt{2\pi} + R_n, \quad 0 < R_n < \frac{1}{12n},$$

we obtain

$$\Delta = (h + k + \frac{1}{2}) \log(h + k) - (h + \frac{1}{2}) \log h - (k + \frac{1}{2}) \log k - R',$$

with $R' < 7/6$. Rearranging gives the desired inequality. \square

Theorem 2.7 (Schur–Sylvester: consecutive integers). *Let $h \geq k$ be natural numbers. Then among the k consecutive integers*

$$h + 1, h + 2, \dots, h + k$$

there is at least one number divisible by a prime $q > k$.

Proof. First, it is enough to prove the theorem for prime values $k = p$. Indeed, assume the statement is already known for primes, and let k be arbitrary. Let p be the largest prime with $p \leq k$, and let $h \geq k$. Then among the p consecutive integers

$$h + 1, h + 2, \dots, h + p$$

there is, by assumption, a number divisible by a prime $q > p$. Since p is the largest prime $\leq k$, the inequality $q > p$ implies $q > k$, and of course the same prime divides one of the numbers

$$h + 1, h + 2, \dots, h + p, \dots, h + k.$$

Thus it remains to prove the theorem for $k = p$ prime.

So let p be prime, let $m = \pi(p)$, and suppose for contradiction that the numbers

$$h + 1, h + 2, \dots, h + p$$

are divisible only by primes $q \leq p$. Then Schur's inequality yields

$$(h + p + \frac{1}{2} - m) \log(h + p) - (h + \frac{1}{2}) \log h - (p + \frac{1}{2}) \log p < \frac{7}{6}.$$

Set

$$S_1 = (h + p + \frac{1}{2} - m) \log(h + p),$$

$$S_2 = (h + \frac{1}{2}) \log h,$$

$$S_3 = (p + \frac{1}{2}) \log p,$$

$$S = S_1 - S_2 - S_3.$$

Then $S < 7/6$. Write $h = Qp$. Using

$$\log(h + p) = \log(Q + 1) + \log p, \quad \log(Q + 1) = \log Q + \log(1 + 1/Q),$$

we obtain

$$\begin{aligned} S_1 &= (h + \frac{1}{2}) \log Q + (h + \frac{1}{2}) \log(1 + 1/Q) + (h + \frac{1}{2} + p - m) \log p + (p - m) \log(Q + 1), \\ S_2 &= (h + \frac{1}{2}) \log Q + (h + \frac{1}{2}) \log p, \\ S_3 &= (p + \frac{1}{2}) \log p. \end{aligned}$$

Hence

$$S = (h + \frac{1}{2}) \log(1 + 1/Q) - (m + \frac{1}{2}) \log p + (p - m) \log(Q + 1). \quad (2.1)$$

Since $h \geq p$, we have $Q \geq 1$, and therefore

$$\log(1 + 1/Q) = \frac{1}{Q} - \frac{1}{2Q^2} + \frac{1}{3Q^3} - \cdots > \frac{1}{Q} - \frac{1}{2Q^2}.$$

It follows that

$$(h + \frac{1}{2}) \log(1 + 1/Q) > (Qp + \frac{1}{2}) \left(\frac{1}{Q} - \frac{1}{2Q^2} \right) = p - \frac{p}{2Q} + \frac{1}{2Q} - \frac{1}{4Q^2} > p - \frac{p}{2Q}.$$

If in (2.1) we leave only the term $(p - m) \log(Q + 1)$ on the smaller side of the inequality, we get

$$(p - m) \log(Q + 1) < \frac{7}{6} + \frac{p}{2Q} + \frac{1}{2} \log p + m \log p - p. \quad (2.2)$$

We now split the proof into two cases.

a) The case $p \geq 29$. We distinguish whether $h \leq 4p$ or $h > 4p$.

If $h \leq 4p$, that is, $Q \leq 4$, then

$$\frac{h + p}{h} = 1 + \frac{1}{Q} \geq 1 + \frac{1}{4} = \frac{5}{4}.$$

Since $h \geq p \geq 29$, the theorem proved earlier on primes in the interval $(x, 5x/4]$ yields a prime P with

$$h < P \leq \frac{5h}{4} \leq h + p.$$

Moreover $p \leq h < P$, so $P > p$. Thus one of the integers $h + 1, \dots, h + p$ is divisible by a prime $P > p$, contradicting our assumption.

Now suppose $h > 4p$, so that $Q > 4$. Then

$$\log(Q + 1) > \log 5 > \frac{5}{8}, \quad \frac{p}{2Q} < \frac{p}{8}.$$

From (2.2) we infer

$$\frac{5}{8}(p - m) < (p - m) \log(Q + 1) < \frac{7}{6} + \frac{p}{8} + \frac{1}{2} \log p + m \log p - p.$$

By the estimate $\pi(x) < \frac{3}{2} \frac{x}{\log x}$, we have

$$m \log p < \frac{3}{2} p,$$

hence

$$m \log p - p < \frac{p}{2}.$$

Therefore

$$\frac{5}{8}(p - m) < \frac{7}{6} + \frac{p}{8} + \frac{1}{2} \log p + \frac{p}{2}.$$

Multiplying by $\frac{8}{5p}$ and rearranging gives

$$\frac{39}{40} < \frac{28}{15p} + \frac{4}{5p} \log p + \frac{8}{5} \cdot \frac{m}{p} < \frac{28}{15p} + \frac{4}{5p} \log p + \frac{12}{5 \log p}. \quad (2.3)$$

The right-hand side is decreasing for $p \geq 29$, so (2.3) would in particular hold for $p = 29$. But this is false; for instance, using $\log(29) < 4$,

$$\frac{28}{15 \cdot 29} + \frac{4}{5 \cdot 29} \log 29 + \frac{12}{5 \log 29} < \frac{28}{435} + \frac{16}{145} + \frac{3}{5} < \frac{39}{40}.$$

This contradiction settles the case $p \geq 29$.

b) The remaining primes. It remains to consider

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23\}.$$

Since $Q \geq 1$, we have $\frac{p}{2Q} \leq \frac{p}{2}$, and from (2.2) we obtain

$$Q + 1 < \exp\left(\frac{1}{p - m} \left(\frac{7}{6} - \frac{p}{2} + (m + \frac{1}{2}) \log p\right)\right).$$

Thus one gets upper bounds K_p for $Q + 1$, namely

p	2	3	5	7	11	13	17	19	23
K_p	4	12	9	9	5	6	5	5	5

Since

$$h + p = Qp + p = (Q + 1)p < K_p p,$$

it is enough, for each fixed p , to check the integers

$$p \leq h < (K_p - 1)p.$$

Moreover, the prime divisors $q > p$ of $h + p$ are exactly the prime divisors $q > p$ of

$$\binom{h + p}{p} = \frac{(h + 1) \cdots (h + p)}{p!}.$$

To avoid checking these finitely many cases by hand, the original thesis uses a computer algebra system such as GP-PARI or GAP. The corresponding pseudo-code is:

```
for h = p, p+1, ..., (K_p-1)p:
  gefunden := FALSE
```

```
PD := primedivisors(binom(h+p,p))
for q in PD:
  if q > p:
    gefunden := TRUE
if gefunden == FALSE:
  print h
```

A computer check shows that no such h occurs. Hence the theorem is proved.

□

Chapter 3

Auxiliary Results from Group Theory

In this chapter we prove several group-theoretic lemmas needed later. We will also prove a theorem on imprimitive groups which says, roughly speaking, that imprimitive groups are contained in wreath products.

3.1 Wreath Products and Imprimitive Groups

Definition 3.1 (Wreath product). *Let G and H be groups, and suppose that H acts on a set Ω . The wreath product $G \wr H$ is the set*

$$\{(f, \sigma) \mid \sigma \in H, f : \Omega \rightarrow G\}$$

with multiplication

$$(f_1, \sigma_1)(f_2, \sigma_2) = (g, \sigma_1\sigma_2), \quad g(\alpha) = f_1(\alpha)f_2(\sigma_1\alpha).$$

Theorem 3.2 (Structure of wreath products). *Suppose H acts on Ω with $|\Omega| = n$. Then $G \wr H$ has a normal subgroup*

$$D = D_1 \times \cdots \times D_n,$$

where each $D_\alpha \cong G$. Moreover,

$$H^* = \{(e, \sigma) \mid \sigma \in H, e(\alpha) = 1 \text{ for all } \alpha \in \Omega\}$$

is a complement of D isomorphic to H . In particular,

$$|G \wr H| = |G|^n |H|.$$

Lemma 3.3 (Action on a Cartesian product). *If G acts on Γ and H acts on Ω , then $G \wr H$ acts on $\Gamma \times \Omega$ by*

$$(\alpha, \beta) \cdot (f, \sigma) = (f(\beta) \cdot \alpha, \sigma \cdot \beta).$$

Definition 3.4 (Imprimitive groups). *Let G act transitively on Ω . We call G imprimitive if there exists a nonempty proper subset $\Delta \subsetneq \Omega$ such that for every $\sigma \in G$ one has either $\Delta \cap \sigma(\Delta) = \emptyset$ or $\sigma(\Delta) = \Delta$. Such a subset Δ is called a block. If no such block exists, the action is called primitive.*

Theorem 3.5 (Imprimitive groups are subgroups of wreath products). *Let G act imprimitively on a finite set Ω , and let Δ be a block. Let*

$$H = \{\sigma \in G \mid \sigma(\Delta) = \Delta\},$$

and write the decomposition into left cosets as $G = \bigcup_{\tau \in L} \tau H$.

(a) *The set Ω decomposes as a disjoint union*

$$\Omega = \bigsqcup_{\tau \in L} \tau(\Delta).$$

(b) *If $|\Delta| = k$ and $|L| = m$, then $|\Omega| = km$ and G is permutation-isomorphic to a subgroup of $S_k \wr S_m$. In particular, $|G|$ divides $m!(k!)^m$.*

(c) *The subgroup H acts transitively on Δ .*

Proof. Part (a) follows from transitivity. Distinct translates of a block are disjoint. Part (b) is obtained by identifying each translate $\tau(\Delta)$ with a copy of a k -element set and comparing the induced action with the standard action of a wreath product on a Cartesian product. Part (c) follows because if $\alpha, \beta \in \Delta$ and $\sigma(\alpha) = \beta$, then $\sigma(\Delta)$ meets Δ , hence $\sigma(\Delta) = \Delta$. \square

3.2 Transitive Groups

Lemma 3.6. *Let G act transitively on Ω , let $U \leq G$, and let $\Delta \subset \Omega$ be an orbit of U . If U acts primitively on Δ and $|\Omega| < 2|\Delta|$, then G acts primitively on Ω .*

Proof. Assume that Ψ is a block for G . By choosing a suitable translate we may assume that $\Lambda := \Psi \cap \Delta$ is nonempty and maximal among intersections of translates of Ψ with Δ . The set Λ is then a block for the action of U on Δ . Since U acts primitively on Δ , either $\Lambda = \Delta$ or $|\Lambda| = 1$. The first case implies $\Delta \subseteq \Psi$, hence $|\Psi| \geq |\Delta|$, contradicting $|\Omega| < 2|\Delta|$ and the divisibility of block sizes. The second case leads to too many distinct translates of Ψ , again contradicting $|\Omega| < 2|\Delta|$. \square

Theorem 3.7 (Transitive groups divisible by a sufficiently large prime). *Let G be a transitive group of degree $n = |\Omega|$, and let p be a prime dividing $|G|$ with $n/2 < p$. Then G is primitive and contains a p -cycle.*

Proof. By Cauchy's theorem, G contains an element of order p . Since $2p > n$, this element must be a single cycle of length p . Let U be the subgroup generated by this p -cycle and let Δ be its support. Then U acts primitively on Δ because $|\Delta| = p$ is prime. Since $n < 2p = 2|\Delta|$, the previous lemma implies that G is primitive. The existence of the p -cycle has already been established. \square

Theorem 3.8 (Jordan). *Let G be a primitive group of degree n . If $|G|$ is divisible by a prime p with*

$$\frac{n}{2} < p < n - 2,$$

then G contains the alternating group A_n .

Chapter 4

The Galois Group of $E_n(x)$ According to Schur

4.1 General Theorems for Computing Galois Groups

Theorem 4.1. *Let K be a number field of degree n with discriminant D , let L be its Galois closure, and let $G = \text{Gal}(L/\mathbb{Q})$. If p is a prime such that $v_p(D) \geq n$, then p divides $|G|$.*

Proof. Let D^* be the discriminant of L . By transitivity of discriminants,

$$D^* = D^{|G|/n} N_{K/\mathbb{Q}}(D_{L/K}),$$

so $v_p(D^*) \geq |G|$. Assume that $p \nmid |G|$. Let \mathfrak{P} be a prime of L above p , with ramification index e , residue degree f , and number of conjugates r . Then $|G| = efr$, so $p \nmid e$. Dedekind's theorem on the different yields $v_{\mathfrak{P}}(\mathfrak{D}_{L/\mathbb{Q}}) = e - 1$, and therefore

$$v_p(D^*) = fr(e - 1) = |G| - |G|/e < |G|,$$

a contradiction. □

Corollary 4.2. *Let K be a number field of degree n with discriminant D , and let p be a prime with $v_p(D) \geq n$ and*

$$\frac{n}{2} < p < n - 2.$$

Let L be the Galois closure of K and assume the Galois group $G = \text{Gal}(L/\mathbb{Q})$ acts transitively of degree n . Then G is either S_n or A_n ; the latter occurs precisely when D is a square.

Proof. By the previous theorem, p divides $|G|$. The group is primitive by the theorem on transitive groups divisible by a large prime, and hence Jordan's theorem implies $A_n \leq G$. Finally, $G = A_n$ exactly when the discriminant is a square. □

Theorem 4.3 (Schur's criterion). *Let*

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$$

be such that:

1. $f(x)$ is irreducible in $\mathbb{Q}[x]$;
2. the discriminant Δ of $f(x)$ is divisible by the n -th power of a prime p ;
3. the constant term a_n is divisible by p but not by p^2 ;
4. modulo p one has

$$\bar{f}(x) \equiv x^k \bar{g}(x) \quad (k > 1),$$

where the discriminant of the monic polynomial $g(x)$ is not divisible by p .

Then the Galois group G of $f(x)$ over \mathbb{Q} has order divisible by p . In particular, if

$$\frac{n}{2} < p < n - 2,$$

then G is either the symmetric or the alternating group; it is alternating if and only if Δ is a square.

Proof. Let D be the discriminant of the number field $\mathbb{Q}(\alpha)$ for a root α of f . We first show that $v_p(\Delta) = v_p(D)$. Since the discriminant of $g(x)$ is not divisible by p , the reduction $\bar{g}(x)$ is separable. Thus x is the only repeated irreducible factor modulo p . Writing

$$f(x) = x^k g(x) - pm(x),$$

Dedekind's criterion shows that it suffices to exclude $m(x) \equiv 0 \pmod{(p, x)}$. But if this congruence held, then $a_n = f(0) = pm(0)$ would be divisible by p^2 , contradicting (3). Hence $v_p(\Delta) = v_p(D) \geq n$. Since f is irreducible, the Galois group is transitive, and the claim follows from the preceding corollary. \square

4.2 Concrete Calculations for $E_n(x)$

Theorem 4.4 (Schur's irreducibility theorem). *A polynomial of the form*

$$f(x) = 1 + g_1 \frac{x}{1!} + g_2 \frac{x^2}{2!} + \cdots + g_{n-1} \frac{x^{n-1}}{(n-1)!} \pm \frac{x^n}{n!}, \quad g_1, \dots, g_{n-1} \in \mathbb{Z},$$

is irreducible over $\mathbb{Q}[x]$.

Proof. Assume that $f(x)$ is reducible and let $A(x)$ be an irreducible factor of degree $k \leq n/2$. After multiplying by $n!$, we may assume that $A(x)$ is monic,

$$A(x) = x^k + a_1 x^{k-1} + \cdots + a_k.$$

The proof proceeds in two steps.

Step 1. Every prime divisor p of a_k satisfies $p \leq k$.

Let α be a root of $A(x)$, and let S be the ring of integers of $\mathbb{Q}(\alpha)$. Since A is the minimal polynomial of α , the norm of α is $\pm a_k$. Thus any prime divisor p of a_k gives rise to a prime ideal \mathfrak{P} dividing both (α) and (p) . Write

$$(\alpha) = \mathfrak{P}^r M, \quad (p) = \mathfrak{P}^s N,$$

with $r, s \geq 1$. Since $s \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = k$, one has $1 \leq r, 1 \leq s \leq k$. Evaluating the scaled polynomial at α and comparing \mathfrak{P} -adic valuations shows that for some $\nu \geq 1$,

$$\nu r \leq s v_{\mathfrak{P}}(\nu!).$$

Using Legendre's formula

$$v_p(\nu!) < \frac{\nu}{p-1}$$

we obtain

$$\nu \leq \nu r \leq s v_{\mathfrak{P}}(\nu!) < \frac{k\nu}{p-1},$$

hence $p-1 < k$ and therefore $p \leq k$.

Step 2. This contradicts the Schur–Sylvester theorem.

Let

$$F(x) = \pm n! f(x) = x^n \pm g_1 n x^{n-1} \pm g_2 n(n-1) x^{n-2} + \dots.$$

For $l = 1, \dots, n$, the coefficient of x^{n-l} is divisible by every prime dividing

$$n(n-1) \cdots (n-l+1).$$

If q divides this product, then modulo q the polynomial $F(x)$ is divisible by x^{n-l+1} . Since $A(x)$ divides $F(x)$ and $\deg A = k$, taking $l = k$ shows that $A(x)$ is divisible by x modulo q . Thus q divides the constant term a_k , and by Step 1, $q \leq k$. Setting $h = n - k$, the k consecutive integers

$$h+1 = n-k+1, \quad h+2 = n-k+2, \quad \dots, \quad h+k = n$$

are divisible only by primes $\leq k$, contradicting the Schur–Sylvester theorem. \square

Lemma 4.5 (The discriminant of $E_n(x)$). *Let D_n be the discriminant of $E_n(x)$. Then:*

1.

$$D_n = (-1)^{\frac{n(n-1)}{2}} (n!)^n.$$

2. *If p is a prime with $n/2 < p < n$, then $v_p(D_n) = n$.*

3. *D_n is a square in \mathbb{Q} if and only if $n \equiv 0 \pmod{4}$.*

4. *No prime $p > n$ divides D_n .*

Proof. Let $B_n(x) = n!E_n(x)$. Since

$$E_n(x) = E_{n-1}(x) + \frac{x^n}{n!},$$

one has

$$B_n(x) = B'_n(x) + x^n.$$

If $\alpha_1, \dots, \alpha_n$ are the roots of $B_n(x)$, then

$$D_n = (-1)^{\frac{n(n-1)}{2}} \prod_i B'_n(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_i (-\alpha_i^n) = (-1)^{\frac{n(n-1)}{2}} (n!)^n.$$

The remaining assertions follow immediately from this formula. \square

Theorem 4.6 (Schur: the Galois group of $E_n(x)$). *The Galois group of $E_n(x)$ over \mathbb{Q} is the alternating group if $n \equiv 0 \pmod{4}$, and otherwise the symmetric group.*

Proof. For $n \leq 7$ the claim can be checked directly with a computer algebra system. Assume $n \geq 8$ and choose a prime p with $n/2 < p < n - 2$ by Tschebyscheff–Bertrand. We apply Schur’s criterion to

$$B_n(x) = n!E_n(x).$$

Condition (1) is Schur’s irreducibility theorem. Condition (2) follows from the discriminant lemma. Condition (3) holds because $B_n(0) = n!$ is divisible by p but not by p^2 . For condition (4), write $m = n - p$. Then the coefficients of $B_n(x)$ satisfy

$$n(n-1)\cdots(n-r+1) \equiv \begin{cases} 0 \pmod{p}, & r \geq n+1-p, \\ m(m-1)\cdots(m-r+1) \pmod{p}, & r < n+1-p. \end{cases}$$

Thus modulo p the polynomial is congruent to x^p times the degree- m polynomial $B_m(x)$, whose discriminant is not divisible by p . Hence Schur’s criterion applies, so the Galois group is either S_n or A_n . The discriminant lemma decides which one occurs. \square

Chapter 5

The Galois Group of $E_n(x)$ According to Coleman

We now compute the Newton polygon of $E_n(x)$.

Lemma 5.1 (Valuation of the factorial). *Let*

$$n = a_0 + a_1p + \cdots + a_s p^s$$

be the p -adic expansion of n . Then

$$v_p(n!) = \frac{n - (a_0 + a_1 + \cdots + a_s)}{p - 1}.$$

Proof. By Legendre's formula,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^s} \right\rfloor.$$

Multiplying by $p - 1$ and telescoping the p -adic digits yields the stated identity. □

Remark 5.2 (Lower convex hull). *Given points $(x_0, y_0), \dots, (x_n, y_n)$ in \mathbb{R}^2 with $x_0 < x_1 < \cdots < x_n$, the lower convex hull can be computed inductively: the first vertex is (x_0, y_0) , and once $(x_{e_{i-1}}, y_{e_{i-1}})$ has been chosen, the next vertex (x_{e_i}, y_{e_i}) is selected so that*

$$\frac{y_{e_i} - y_{e_{i-1}}}{x_{e_i} - x_{e_{i-1}}} \leq \frac{y_j - y_{e_i}}{x_j - x_{e_i}} \quad \text{for all } x_j > x_{e_{i-1}}.$$

Figure 5.1 illustrates this construction.

Theorem 5.3 (The Newton polygon of $E_n(x)$). *Let*

$$n = b_1 p^{k_1} + b_2 p^{k_2} + \cdots + b_s p^{k_s}$$

be the p -adic expansion of n , with $k_1 > k_2 > \cdots > k_s$ and $0 < b_i < p$. Then the vertices of the

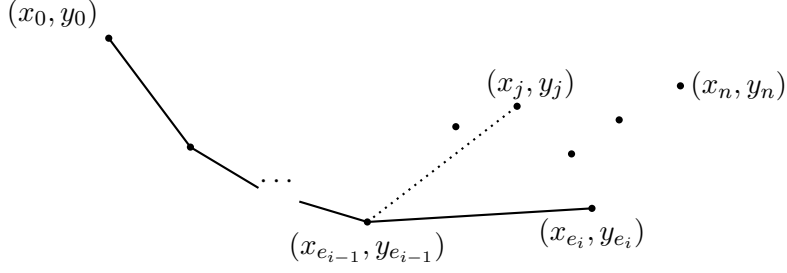


Figure 5.1: Lower convex hull.

Newton polygon of $E_n(x)$ are

$$(x_i, y_i), \quad x_i = b_1 p^{k_1} + \cdots + b_i p^{k_i}, \quad y_i = v_p\left(\frac{1}{x_i!}\right), \quad 1 \leq i \leq s.$$

Proof. By the description of the lower convex hull, it suffices to verify the slope inequalities. If $x_j = j$ with $x_{i-1} < j \leq n$, then the p -adic expansion of j has the form

$$j = b_1 p^{k_1} + \cdots + b_{i-1} p^{k_{i-1}} + c_r p^r + \cdots + c_0, \quad r < k_i.$$

Using the factorial valuation lemma, one computes

$$\frac{y_j - y_{i-1}}{x_j - x_{i-1}} = \frac{x_{i-1} - j - (c_0 + \cdots + c_r)}{(p-1)(j - x_{i-1})}$$

and

$$\frac{y_i - y_{i-1}}{x_i - x_{i-1}} = \frac{1 - p^{k_i}}{p^{k_i}(p-1)}.$$

The desired inequality is equivalent to

$$j - x_{i-1} \leq p^{k_i}(c_0 + \cdots + c_r),$$

which is clear from the expansion of $j - x_{i-1}$. \square

Corollary 5.4. *If p^m divides n , then p^m divides the degree of every irreducible factor of $E_n(x)$ over \mathbb{Q}_p .*

Proof. Every slope denominator occurring in the Newton polygon is of the form $p^{k_i}(p-1)$, and if $p^m \mid n$, then $m \leq k_i$ for each i . The main theorem on Newton polygons therefore implies that each irreducible factor degree is divisible by p^m . \square

Corollary 5.5. *If $p^k \leq n$, then p^k divides the degree of the splitting field of $E_n(x)$ over \mathbb{Q}_p .*

Proof. The denominator of the slope of the first edge is divisible by p^k , so the main Newton polygon theorem implies that the local Galois group order is divisible by p^k . \square

Theorem 5.6. *The exponential Taylor polynomial $E_n(x)$ is irreducible over \mathbb{Q} .*

Proof. Let $n = \prod_i p_i^{k_i}$ be the prime factorization of n , and let $f(x)$ be an irreducible factor of $E_n(x)$ over \mathbb{Q} . Fix p_i . Over \mathbb{Q}_{p_i} the polynomial $f(x)$ factors into irreducibles whose degrees are all divisible by $p_i^{k_i}$ by the previous corollary. Hence $p_i^{k_i} \mid \deg f(x)$. Since this holds for every prime power dividing n , we obtain $n \mid \deg f(x)$. But $\deg f \leq \deg E_n = n$, so $\deg f = n$ and $E_n(x)$ is irreducible. \square

Theorem 5.7. *Let p be a prime with $n/2 < p \leq n$, and let G be the Galois group of $E_n(x) = 0$ over \mathbb{Q} . Then G contains a p -cycle and is primitive.*

Proof. Since $p \leq n$, the previous corollary shows that p divides the degree of the splitting field of $E_n(x)$ over \mathbb{Q}_p , hence also the degree of the global splitting field, which is $|G|$. By irreducibility, G is transitive. The theorem on transitive groups divisible by a sufficiently large prime now shows that G is primitive and contains a p -cycle. \square

Lemma 5.8. *Let G be the Galois group of $E_n(x) = 0$ over \mathbb{Q} . Then $A_n \leq G$.*

Proof. For $n \leq 7$ this can be checked directly with a computer algebra system such as GP-PARI. For $n = 3$, for example, the original thesis gives the command

```
polgalois(1/6*x^3 + 1/2*x^2 + x + 1)
```

For $n \geq 8$, Tschebyscheff–Bertrand provides a prime p with $n/2 < p < n - 2$. The preceding theorem shows that G is primitive and contains a p -cycle. Jordan’s theorem then yields $A_n \leq G$. \square

Theorem 5.9 (The Galois group of the exponential Taylor polynomial). *Let G be the Galois group of $E_n(x) = 0$ over \mathbb{Q} . Then*

$$G = S_n \quad \text{if } n \not\equiv 0 \pmod{4}, \quad G = A_n \quad \text{if } n \equiv 0 \pmod{4}.$$

Proof. From the Schur part we know that

$$\text{Disc}(E_n) = (-1)^{\frac{n(n+1)}{2}} (n!)^n,$$

which is a square exactly when $n \equiv 0 \pmod{4}$. Since $A_n \leq G$, the discriminant criterion from Galois theory implies the stated dichotomy. \square

Chapter 6

Observations on $C_n(x)$

We begin with a property of composite polynomials; compare also Odoni and Geissler–Klüners.

Theorem 6.1 (Imprimitivity and $f(x) = g(h(x))$). *Let k be a field of characteristic 0, let $f(x)$ be an irreducible polynomial in $k[x]$ with root set Ω_f in an algebraic closure, let $K = k(\Omega_f)$ be the splitting field, and let $G = \text{Gal}(K/k)$. Then the following are equivalent:*

- (1) *There exist polynomials $g(x) \in K[x]$ and $h(x) \in k[x]$, both of degree at least 2, such that $f(x) = g(h(x))$.*
- (2) *(a) G is imprimitive with a block Δ ;*
(b) if $H = \{\sigma \in G \mid \sigma(\Delta) = \Delta\}$, F is the fixed field of H , and $b \in \Delta$, then

$$\text{Irr}(b, F, x) = h(x) - a$$

for some polynomial $h(x) \in k[x]$ and some $a \in F$.

Proof. Assume first that $f(x) = g(h(x))$. Let Ω_g be the root set of g in K ; then

$$f(x) = \prod_{a \in \Omega_g} (h(x) - a).$$

For each $a \in \Omega_g$, let Ω_a be the root set of $h(x) - a$. Because the factors are separable, the sets Ω_a are nonempty proper subsets of Ω_f , and for every $\tau \in G$ one has

$$\tau(\Omega_a) = \Omega_{\tau(a)}.$$

Hence each Ω_a is a block. Choosing $\Delta = \Omega_a$ and letting H be its stabilizer, transitivity of H on Δ implies that $h(x) - a$ is irreducible over the fixed field F of H , so it is the minimal polynomial of any $b \in \Delta$.

Conversely, suppose (2) holds. By the block decomposition theorem,

$$\Omega_f = \bigsqcup_{\tau \in L} \tau(\Delta)$$

for a set L of left coset representatives of H in G . If $b \in \Delta$ and $\text{Irr}(b, F, x) = h(x) - a$, then for every $\tau \in L$ the polynomial $h(x) - \tau(a)$ has root set $\tau(\Delta)$. Therefore

$$f(x) = \prod_{\tau \in L} (h(x) - \tau(a)) = g(h(x))$$

with

$$g(x) = \prod_{\tau \in L} (x - \tau(a)).$$

□

Remark 6.2. *In general, conditions (a) and (b) in part (2) are not equivalent. Here is a counterexample. Let z_1, z_2, z_3, z_4 be transcendental over \mathbb{C} , let*

$$K := \mathbb{C}(z_1, z_2, z_3, z_4),$$

and let the dihedral group D_8 , generated by

$$\tau = (1\ 2)(3\ 4), \quad \sigma = (1\ 2\ 3\ 4),$$

act transitively on the root set

$$\Omega_f := \{z_1, z_2, z_3, z_4\}$$

of

$$f(x) = (x - z_1) \cdots (x - z_4).$$

Let k be the fixed field of D_8 under this action. Then $D_8 = \text{Gal}(K/k)$. One checks easily that

$$\Delta = \{z_1, z_3\}$$

is a block of Ω_f , so D_8 acts imprimitively on Ω_f and condition (2a) is satisfied.

Now let

$$H = \{\alpha \in D_8 \mid \alpha(\Delta) = \Delta\},$$

and let F be the fixed field of H . Since H acts transitively on Δ by Theorem 3.2, the polynomial

$$\prod_{b_0 \in \Delta} (x - b_0) = (x - z_1)(x - z_3)$$

is irreducible in $F[x]$, hence it is the irreducible polynomial of $b := z_1$ over F .

However, this polynomial is not of the form

$$h(x) - a = (x - z_1)(x - z_3) = x^2 - (z_1 + z_3)x + z_1 z_3$$

with $h(x) \in k[x]$. For otherwise we would have

$$h(x) = x^2 - (z_1 + z_3)x,$$

and therefore $z_1 + z_3 \in k = K^{D_8}$. But this is false, since for example

$$\sigma(z_1 + z_3) = z_2 + z_4 \neq z_1 + z_3.$$

Indeed, equality would imply $z_1 + z_3 - z_2 - z_4 = 0$, contradicting the transcendence of the z_i over \mathbb{C} .

Corollary 6.3. *Let k be a field of characteristic 0, and let $f(x) = g(h(x)) \in k[x]$ be irreducible, with $\deg g = l \geq 2$ and $\deg h = m \geq 2$. If K is the splitting field of f and $G = \text{Gal}(K/k)$, then G is a subgroup of $S_m \wr S_l$.*

Proof. By the theorem, G is imprimitive with a block of size m . The subgroup statement is therefore an immediate consequence of the characterization of imprimitive groups as subgroups of wreath products. \square

Corollary 6.4. *The Galois group of the Taylor polynomial*

$$C_n(x) = \sum_{k=0}^n \frac{x^{2k}}{(2k)!}$$

over \mathbb{Q} is a subgroup of $S_2 \wr S_n$.

Proof. By Schur's irreducibility theorem, this polynomial is irreducible. Apply the previous corollary to the decomposition $C_n(x) = g(h(x))$ with

$$g(x) = \sum_{k=0}^n \frac{x^k}{(2k)!}, \quad h(x) = x^2.$$

\square

Lemma 6.5. *Let $A = \{a_1, \dots, a_n\} \subset k^*$ be a finite set such that for every pair of disjoint subsets $B, C \subset A$ the element*

$$\prod_{b \in B} b \prod_{c \in C} c^{-1}$$

is not a square in k . Let $\Lambda = \{\alpha_1, \dots, \alpha_n\}$, where α_i is a root of $x^2 - a_i$, and let $\Lambda_i = \Lambda \setminus \{\alpha_i\}$. Then for every i :

- 1) $x^2 - a_i$ is irreducible over $k(\Lambda_i)$;
- 2) $k(\alpha_i) \cap k(\Lambda_i) = k$;
- 3) the Galois group of $k(\Lambda)/k$ is $C_2^n = C_2 \times \dots \times C_2$.

Proof. Proceed by induction on n . The case $n = 1$ is clear. For the induction step, one first shows that $x^2 - a_{n+1}$ remains irreducible over $k(\alpha_1, \dots, \alpha_n)$; otherwise one would obtain either that a_{n+1} itself is a square in $k(\alpha_1, \dots, \alpha_{n-1})$ or that a_{n+1}/a_n is such a square, contradicting the induction hypothesis applied to a suitable n -element subset. Hence adjoining the square roots doubles the degree at each step, and a basis is given by all squarefree monomials in the

α_i . The intersection statement follows from linear independence in that basis, and the Galois group is therefore the direct product of the individual quadratic Galois groups. \square

Remark 6.6. *The hypotheses in the previous lemma are necessary. For example,*

$$(x^2 - 2^2 \cdot 5)(x^2 - 3^2 \cdot 5)$$

has splitting field $\mathbb{Q}(\sqrt{5})$. Although both $2^2 \cdot 5$ and $3^2 \cdot 5$ are non-squares in \mathbb{Q} , their quotient is a square, and the Galois group is only C_2 , not $C_2 \times C_2$.

Remark 6.7. *The condition*

$$B, C \subset A, B \cap C = \emptyset \implies \prod_{b \in B} b \prod_{c \in C} c^{-1} \text{ is not a square in } k^*$$

is equivalent to the simpler condition that for every subset $B \subset A$, the product $\prod_{b \in B} b$ is not a square in k^ .*

Remark 6.8. *Let $f(x) \in k[x]$ be separable of degree n and Galois group S_n over k . Let $A = \{\alpha_1, \dots, \alpha_n\}$ be the root set of f , and let $K = k(A)$ be the splitting field. If for every subset $B \subset A$ the product $\prod_{b \in B} b$ is not a square in K , then the polynomial $f(x^2)$ has Galois group $S_2 \wr S_n$ over k .*

Proof. Since S_n acts transitively on the roots of f , the polynomial f is irreducible over k . By assumption, each $x^2 - \alpha_i$ is irreducible over K , and by the previous lemma the extension obtained by adjoining the square roots of the roots has Galois group C_2^n over K . This is precisely the splitting field of $f(x^2)$. Hence the total degree is $2^n n!$, which equals the order of $S_2 \wr S_n$. Since the earlier corollary already places the Galois group inside the wreath product, equality follows. \square

It is unclear whether the last remark can be used to prove that $C_n(x)$ has Galois group $S_2 \wr S_n$ over \mathbb{Q} . Computations with GP-PARI do, however, suggest that the polynomial

$$\sum_{k=0}^n \frac{x^k}{(2k)!}$$

has Galois group S_n over \mathbb{Q} .

In view of the difficulties one encounters when trying to compute the discriminant of $C_n(x)$, it is worth pointing out that the discriminant of $C_n(x)$ is never a square in \mathbb{Q} . For this we need the following result.

Lemma 6.9. *Let $f(x), g(x) \in k[x]$, let $h(x) = f(g(x))$, and let Δ_f, Δ_h denote the discriminants of f and h , respectively. Then*

$$\Delta_h = \Delta_f^m \cdot \text{Res}(h, g') \cdot (-1)^{\frac{mn(mn-2+n)}{2}},$$

where $m = \deg g$ and $n = \deg f$.

Proof. Let α run through all roots of h and β through all roots of f . Then

$$\Delta_f = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{\beta} f'(\beta).$$

Since $0 = h(\alpha) = f(g(\alpha))$, we obtain

$$\prod_{\alpha} f'(g(\alpha)) = \prod_{\beta} f'(\beta)^{\deg g} = \prod_{\beta} (f'(\beta))^m.$$

Hence

$$\begin{aligned} \Delta_h &= (-1)^{\frac{mn(mn-1)}{2}} \operatorname{Res}(h, h') = (-1)^{\frac{mn(mn-1)}{2}} \prod_{\alpha} f'(g(\alpha)) g'(\alpha) \\ &= (-1)^{\frac{mn(mn-1)}{2}} \left(\prod_{\beta} f'(\beta) \right)^m \cdot \prod_{\alpha} g'(\alpha) \\ &= (-1)^{\frac{mn(mn-1)}{2}} \Delta_f^m \cdot \operatorname{Res}(h, g') \cdot \left((-1)^{\frac{n(n-1)}{2}} \right)^m, \end{aligned}$$

which is exactly the stated formula. □

Corollary 6.10. *Let*

$$f(x) = (2n)! \sum_{k=0}^n \frac{x^k}{(2k)!}, \quad h(x) = (2n)! \sum_{k=0}^n \frac{x^{2k}}{(2k)!},$$

and let Δ_f and Δ_h be the discriminants of $f(x)$ and $h(x)$, respectively. Then

$$\Delta_h = \Delta_f^2 \cdot 2^{2n} \cdot (2n)! \cdot (-1)^{n(3n-2)},$$

and Δ_h is not a square in \mathbb{Z} .

Proof. Here $g(x) = x^2$ in the preceding lemma, and since

$$\operatorname{Res}(h, g') = \prod_{\alpha} g'(\alpha) = \prod_{\alpha} 2\alpha = 2^{2n} \cdot h(0) = 2^{2n} (2n)!,$$

it follows that

$$\Delta_h = \Delta_f^2 \cdot 2^{2n} \cdot (2n)! \cdot (-1)^{n(3n-2)}.$$

By Tschebyscheff's theorem there exists a prime p with $n < p < 2n$, hence $v_p((2n)!) = 1$. Therefore

$$v_p(\Delta_h) = 2v_p(\Delta_f) + v_p((2n)!) = 2v_p(\Delta_f) + 1$$

is odd, so Δ_h cannot be a square in \mathbb{Q} . □

From now on we write

$$D_n(x) = (2n)! \sum_{k=0}^n \frac{x^k}{(2k)!}, \quad S_n(x) = (2n+1)! \sum_{k=0}^n \frac{x^k}{(2k+1)!}.$$

By Schur's irreducibility theorem, $D_n(x^2)$ is irreducible over $\mathbb{Q}[x]$, and therefore so is $D_n(x)$. (In a later paper Schur showed, by methods similar to those used in his irreducibility theorem, namely with the aid of number-theoretic results, that $S_n(x)$ is also irreducible over $\mathbb{Q}[x]$. A check for small degrees with GP-PARI suggests that $S_n(x)$ likewise has symmetric Galois group. Here, however, we only discuss those properties of $S_n(x)$ that help us understand the polynomials $D_n(x)$ better.)

Lemma 6.11 (The leftmost side of the Newton polygon of $D_n(x)$). *Let p be a prime in the interval $n/2 < p < n$. Then the leftmost side of the Newton polygon has length p and slope $-2/p$.*

Proof. Multiplying $D_n(x)$ by $(2n)!^{-1}$ merely shifts the Newton polygon downward, so it suffices to compute the first side of

$$\frac{1}{(2n)!}D_n(x) = \sum_{j=0}^n \frac{x^j}{(2j)!}.$$

As one sees by comparing slopes in the polygon, it is enough to show that

$$\frac{v_p((2j)!)}{j} \geq \frac{2}{p} \quad (j = 1, 2, \dots, n).$$

Now

$$v_p((2j)!) = \left\lfloor \frac{2j}{p} \right\rfloor + \left\lfloor \frac{2j}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{2j}{p^r} \right\rfloor$$

for some natural number r . It is enough to show that $r = 1$, because then

$$v_p((2j)!) = \left\lfloor \frac{2j}{p} \right\rfloor \leq \frac{2j}{p}.$$

By the assumptions on j , n , and p , we have

$$2j \leq 2n < 4p < p^2,$$

hence $2j/p^2 < 1$, so $\lfloor 2j/p^2 \rfloor = 0$, and therefore $r = 1$. □

Theorem 6.12. *The Galois group of $D_n(x)$ is either the alternating group or the symmetric group.*

Proof. Since $D_n(x)$ is irreducible over $\mathbb{Q}[x]$, its Galois group is transitive. By the previous lemma and the main theorem on Newton polygons, the order of the group is divisible by a prime p in the interval $n/2 < p < n$. By Theorem 3.3 on transitive groups whose order is divisible by a large prime, such a group is already primitive. Jordan's theorem then yields the claim. □

Lemma 6.13. *Let p be a prime with $n < p < 2n$, and put*

$$r = n - \frac{p+1}{2}, \quad t = n - \frac{p-1}{2}.$$

Then

$$D_n(x) \equiv x^{\frac{p+1}{2}} S_r(x) \pmod{p}, \quad (6.1)$$

$$S_n(x) \equiv x^{\frac{p-1}{2}} D_t(x) \pmod{p}. \quad (6.2)$$

Proof. We prove only the first statement; the second is similar. We have

$$D_n(x) = x^n + 2n(2n-1)x^{n-1} + 2n(2n-1)(2n-2)(2n-3)x^{n-2} + \cdots + (2n)!.$$

For $0 \leq l \leq n$, the various terms in $D_n(x)$ are of the form

$$2n(2n-1) \cdots (2l+1)x^{n-l}.$$

Hence

$$\begin{aligned} D_n(x) &\equiv x^n + 2n(2n-1)x^{n-1} + 2n(2n-1)(2n-2)(2n-3)x^{n-2} + \cdots + (2n)! \pmod{p} \\ &\equiv x^{\frac{p+1}{2}} (x^r + (2r+1)(2r)x^{r-1} + (2r+1)(2r)(2r-1)(2r-2)x^{r-2} + \cdots + (2r+1)!) \\ &\equiv x^{\frac{p+1}{2}} S_r(x) \pmod{p}. \end{aligned}$$

□

Theorem 6.14. *Retain the notation of the previous lemma. Let α be a root of $D_n(x)$, let Δ_n be the discriminant of $D_n(x)$, let d_n be the discriminant of $\mathbb{Q}(\alpha)$, and let R be the ring of integers of $\mathbb{Q}(\alpha)$. If one of the following equivalent conditions holds:*

1. *besides x , the polynomial $D_n(x)$ has no multiple roots modulo p ;*
2. *the polynomial $S_r(x)$ has no multiple roots modulo p ;*
3. *the discriminant of $S_r(x)$ is not divisible by p ,*

then the Galois group of $D_n(x)$ over \mathbb{Q} is the symmetric group.

Proof. The equivalence of (1) and (2) is proved with the aid of formal differentiation, using the product rule and equation (6.1). The equivalence of (2) and (3) is standard and rests on the fact that the discriminant of a polynomial can be written as

$$\left(\prod_{i < j} (\alpha_i - \alpha_j) \right)^2,$$

where the α_i run over the roots of the polynomial.

Now assume that (1) holds. Since the constant coefficient $D_n(0) = (2n)!$ is divisible by p but not by p^2 , condition 2(a) in Dedekind's criterion is satisfied with $f_s(x) = x$ and $e_s = (p+1)/2$, whereas 2(b) is not. By that criterion,

$$v_p(\Delta_n) = v_p(d_n).$$

Since $d_n = |R : \mathbb{Z}[\alpha]| \cdot \Delta_n$, it follows that $|R : \mathbb{Z}[\alpha]|$ is not divisible by p . By the Kummer-Dedekind factorization theorem, there exists a prime ideal P of R such that p factors with ramification index $e = (p + 1)/2$ and residue degree $f = \deg x = 1$ over this prime ideal.

Clearly $e = (p + 1)/2$ is not divisible by p . Hence, by Dedekind's theorem on the different and the discriminant,

$$v_P(d_n) = e - 1 = \frac{p - 1}{2}.$$

Therefore the highest power of p occurring in d_n is

$$p^{f(e-1)} = p^{1 \cdot \frac{p-1}{2}} = p^{\frac{p-1}{2}},$$

that is,

$$v_p(d_n) = \frac{p - 1}{2}.$$

Now one may choose the prime p in the interval $n < p < 2n$ in such a way, using a theorem of Robert Breusch refining the ideas of Tschebyscheff, that $(p - 1)/2$ is odd. Then $v_p(d_n)$ is odd as well, and so d_n cannot be a square in \mathbb{Q} . Consequently the Galois group is the symmetric group rather than the alternating group. \square

Bibliography

Bibliography

- [1] I. Schur, *Beispiele für Gleichungen ohne Affekt*, Gesammelte Abhandlungen, Vol. III, No. 38, 280–285, 1920.
- [2] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I*, Gesammelte Abhandlungen, Vol. III, No. 64, 140–151, 1929.
- [3] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen II*, Gesammelte Abhandlungen, Vol. III, No. 65, 370–391, 1929.
- [4] I. Schur, *Gleichungen ohne Affekt*, Gesammelte Abhandlungen, Vol. III, No. 67, 191–197, 1930.
- [5] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Gesammelte Abhandlungen, Vol. III, No. 70, 227–233, 1931.
- [6] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, Journal de Théorie des Nombres de Bordeaux **17** (2005), 517–525.
- [7] M. Hall, *Theory of Groups*, Macmillan, 1959.
- [8] C. Jordan, *Sur la limite de transitivité des groupes non alternes*, Bull. Soc. Math. France **1** (1872/73), 40–71.
- [9] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Vol. I.
- [10] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, Enseign. Math. (2) **33** (1987), no. 3–4, 183–189.
- [11] R. W. K. Odoni, *The Galois Theory of Iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), 385–414.
- [12] F. Q. Gouvêa, *p -adic Numbers*, second edition, Springer, 1997.
- [13] GP/PARI, Version 2.3.4.
- [14] B. Huppert, *Endliche Gruppen I*, Springer, 1967.
- [15] S. Lang, *Algebraic Number Theory*, Springer, second edition, 1970.
- [16] S. Lang, *Algebra*, Graduate Texts in Mathematics, revised 3rd edition, Springer, 2002.

- [17] E. Artin, *Galois Theory*, Dover, 1998.
- [18] A. Leutbecher, *Zahlentheorie, Eine Einführung in die Algebra*, Springer, 1991.
- [19] P. Schmid, *Algebraische Zahlentheorie*, lecture notes, Tübingen, Winter Semester 2008/2009.
- [20] M. Kölle, *Zur Berechnung von Galoisgruppen globaler Polynome durch Newton-Polygone*, dissertation, University of Tübingen, 2002.
- [21] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.
- [22] K. Geissler and J. Klüners, *Galois Group Computation for Rational Polynomials*, J. Symbolic Computation (2000), Theorem 3.1.

Acknowledgements

First of all, I would like to thank my family, who have always supported me in what I do. My former teacher Klaus Pullmann supported me greatly both during school and during my studies, and I would like to thank him sincerely. I would also like to thank my supervisor Prof. Dr. M. Lehn, who always helped me whenever I got stuck.

Declaration

I hereby declare that I prepared this diploma thesis independently and used only the aids listed in the bibliography.

Mainz, 27 May 2010

Orges Leka