surfaces of order t, the image of C_{2s-1} for a particular surface is a conical curve of order $(2s-1)t$.

In S_r, the image of any point on the base M_{s2} or M_{t2} is a conic. The lines joining points of M to a particular point of f_1 form a conical primal with a point vertex. It is met by the corresponding primal of the second pencil in a manifold $M^{r-2}_{(3s-2)t}$ or $M^{r-2}_{(2s-1)t}$ according as there is contact or not.

UNIVERSITY OF BUFFALO

NOTE ON SOME EQUATIONS WITHOUT AFFECT*

BY SAUNDERS MACLANE

A numerical equation of degree greater than 4 certainly cannot be solved by radicals if it is "without affect"; that is, if its Galois group is the symmetric group. Hence it is of interest to construct explicitly such equations. A number of such constructions have been developed,† many of them intrinsically related to certain prime-ideal decompositions. Hence the Newton polygon construction for prime ideals and the related Eisenstein irreducibility criterion are relevant, and can be used systematically to give new proofs for several known constructions (Theorem 2) and for some new equations without affect (Theorems 1 and 2 and generalizations). The advantages lie in the uniform procedure and in the ease of the explicit construction of Theorem 1.

THEOREM 1. *Let p, q, and r be rational primes and construct*

$$(1)\qquad f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n, \qquad (n \geqq 4),$$

with rational integral coefficients a_i such that: (I) *each a_i is divisible by r, but a_n is not divisible by r^2*; (II) *each a_i is divisible by q, and a_n but not a_{n-1} is divisible by q^2*; (III) *the highest power e_i such that a_i is divisible by p^{e_i} satisfies*

$$(2)\qquad e_1 \geqq 1, \qquad e_2 = 1, \qquad e_3 \geqq 2, \qquad e_i - e_{i-1} > e_{i-1} - e_{i-2},$$

* Presented to the Society, April 10, 1936, and subsequently extended.

† Ph. Furtwängler, *Ueber Kriterien für irreduzible und für primitive Gleichungen und über die Aufstellung affektfreier Gleichungen*, Mathematische Annalen, vol. 85 (1922), pp. 34–40.

for $i=4, 5, \cdots, n$. Then the Galois group of $f(x)$, considered as a permutation group G on the roots of $f(x)$, is the symmetric group.[*]

The assumption I of the theorem is exactly the condition under which the *Eisenstein irreducibility Theorem*[†] asserts the irreducibility of $f(x)$. Hence the group G is transitive.

In the field $R(\alpha)$, obtained by adjoining to the rational field R a root α of $f(x)$, certain prime ideal factors of a prime q may be found thus: Plot in a plane the points $A_i=(i, d_i)$, where d_i is the exact power to which a_i is divisible by q. The convex broken line which joins $A_0=(0, 0)$ to A_n, which has vertices only at certain of the points A_i, and which passes above none of these points is the *Newton Polygon* of $f(x)$. If a side A_iA_j of this polygon has a positive slope $e/(j-i)$, with e prime to $(j-i)$, then q is known to have[‡] a corresponding prime factor Q in $R(\alpha)$ such that q is divisible by Q^{j-i} and no higher power, and α is divisible by Q^e and no higher power.

By hypothesis II the polygon for q has two sides A_0A_{n-1} and $A_{n-1}A_n$. If Q is the prime ideal corresponding to the second side, then $q\equiv 0$ and $\alpha\equiv 0 \pmod{Q}$, $q\not\equiv 0 \pmod{Q^2}$. Hence the equation

$$\begin{aligned} f_1(x) &= f(x)/(x-\alpha) \\ &= x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \cdots + b_{n-1} \end{aligned} \tag{3}$$

has coefficients b_i in the field $R(\alpha)$,

$$b_i = \alpha^i + a_1\alpha^{i-1} + a_2\alpha^{i-2} + \cdots + a_i, \qquad (i = 1, \cdots, n-1), \tag{4}$$

whence, by II, $b_i\equiv 0 \pmod{Q}$. But $a_{n-1}\not\equiv 0 \pmod{Q^2}$, so that $b_{n-1}\not\equiv 0 \pmod{Q^2}$. Hence the Eisenstein criterion for the prime ideal Q in $R(\alpha)$ applies to $f_1(x)$ and shows it irreducible. Therefore the subgroup of G corresponding to the field $R(\alpha)$ (that is,

[*] This construction avoids the Cauchy-Sylow Theorem and the Tchebichef Theorem on the existence of primes between $n/2$ and n, thus simplifying a similar method due to M. Bauer, *Ueber Gleichungen ohne Affekt*, Journal für Mathematik, vol. 132 (1907), pp. 33–35.

[†] B. L. van der Waerden, *Moderne Algebra*, vol. 1, p. 77.

[‡] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Mathematische Annalen, vol. 99 (1928), pp. 84–117.

the subgroup leaving $\alpha=\alpha_1$ fixed) is transitive* on the remaining roots $\alpha_2, \cdots, \alpha_n$.

To decompose p in $R(\alpha)$, form the Newton polygon for the points $B_0=(0, 0)$ and $B_i=(i, e_i)$ representing the powers p^{e_i} in a_i. By III this polygon has the sides B_0B_1, $B_2B_3, \cdots, B_{n-1}B_n$. The last side $B_{n-1}B_n$ has a slope e_n-e_{n-1} and so corresponds to a prime ideal P with $p\equiv 0 \pmod{P}$, $p\not\equiv 0 \pmod{P^2}$, $\alpha\equiv 0 \pmod{P^{e_n-e_{n-1}}}$. By (2) and (4), $b_1=\alpha+a_1\equiv 0 \pmod{P}$. Furthermore, for any $i>1$, P^{e_i} is the highest power of P dividing b_i, for in the expression (4) for b_i the first term is divisible by a higher power of P than the third term, while by (2) any other term $a_j\alpha^{i-j}$ is divisible by a higher power of P than the subsequent term $a_{j+1}\alpha^{i-j-1}$. Thus b_i is divisible by the power P^{e_i} dividing the last term, and $f_1(x)$ satisfies with respect to P the analog of III. The argument can be repeated on $f_2(x)=f_1(x)/(x-\alpha_2)$, and so on. By choosing each time a prime ideal corresponding to the steepest remaining side of the polygon, we finally obtain a prime ideal $\mathfrak{p}$ in the field $K=R(\alpha_1, \cdots, \alpha_{n-2})$ such that the remaining factor of $f(x)$,

$$f_{n-2}(x) = (x-\alpha_{n-1})(x-\alpha_n) = x^2+c_1x+c_2,$$

has coefficients c_1 and c_2 in K divisible by $\mathfrak{p}^{e_1}$ and $\mathfrak{p}^{e_2}$, respectively. Since $e_1\geqq e_2=1$, $f_{n-2}(x)$ is irreducible by the Eisenstein criterion. The group of $f_{n-2}(x)$ over K is therefore transitive, so that G contains a transposition (α_{n-1}, α_n). This fact, coupled with the transitivity of G and of the subgroup of G leaving $\alpha_1=\alpha$ fixed, suffice† to make G the symmetric group.

Conditions I, II, and III of this theorem specify essentially that r be a power of a prime ideal in $R(\alpha)$, that a factor of q in $R(\alpha_1)$ be a power of a prime ideal in $R(\alpha_1, \alpha_2)$, that a factor of p in K be a power of a prime ideal in $K(\alpha_{n-1})$. Other conditions can have the same ideal-theoretic effect.

THEOREM 2. *Theorem* 1 *remains valid when* I *is replaced by*

* Therefore any irreducible equation satisfying II is primitive. This proves a primitivity criterion due to Furtwängler, op. cit., p. 37.

† The proof is essentially that in van der Waerden, op. cit., p. 191. If p, q, and r are sufficiently large, Theorem 1 could also be established by a theorem of Wegner connecting the prime decomposition and the Galois group; U. Wegner, *Zur Theorie der affektlosen Gleichungen*, Mathematische Annalen, vol. 111 (1935), pp. 738–742.

one of the following conditions; (Ia) $f(x)$ *is irreducible* (mod r); (Ib) r *is a power of a prime ideal in the ring of polynomials* $R[x]$ modulo $f(x)$. *Likewise* II *or* III *may be replaced respectively by the alternatives*

$$\text{(IIa)} \qquad a_1 \not\equiv 0 \pmod{q}, \quad a_2 \equiv a_3 \equiv \cdots \equiv a_n \equiv 0 \pmod{q}, \quad a_n \not\equiv 0 \pmod{q^2};$$

$$\text{(IIb)} \qquad f(x) \equiv \phi(x)(x-c) \pmod{q}, \qquad (\phi(x) \text{ irreducible mod } q);$$

$$\text{(IIIa)} \qquad f(x) \equiv x^2\psi_1(x)\cdots\psi_t(x) \pmod{p}, \quad a_n \not\equiv 0 \pmod{p^2},$$

where x *and the* $\psi_i(x)$ *are distinct irreducible polynomials* (mod p);

$$\text{(IIIb)} \qquad f(x) \equiv \phi(x)\psi_1(x)\cdots\psi_t(x) \pmod{p},$$

where the $\psi_i(x)$ *are distinct irreducible polynomials of odd degree* (mod p), *and* $\phi(x)$ *is irreducible and of degree two* (mod p).

Conditions Ia, IIb, and IIIb combined give a construction for equations without affect due essentially to Bauer.* On the other hand, conditions I, IIa, and IIIa, with $t=n-2$, generalize a construction of Perron,† who avoided group theoretic arguments by using conditions on $n-1$ primes instead of on three primes, p, q, and r. Other alternatives to conditions I, II, and III are possible.

Proof. The alternative conditions will give the same properties of the group G as did the original I, II, and III. Condition Ia immediately implies the irreducibility of $f(x)$ and hence the transitivity of G. Condition Ib, by a generalization of the Eisenstein criterion, yields‡ the same conclusion.

We now use another prime ideal construction. If $f(x)$ has a non-multiple irreducible factor $\phi(x)$ (mod q), then there is a prime ideal $Q=(q, \phi(\alpha))$ in $R(\alpha)$ which divides q to the first power only.§ In particular, condition IIa gives $f(x) \equiv x^{n-1}(x+a_1)$

* M. Bauer, *Ganzzählige Gleichungen ohne Affekt*, Mathematische Annalen, vol. 64 (1907), pp. 325–327. Also in van der Waerden, op. cit., p. 191.

† O. Perron, *Ueber Gleichungen ohne Affekt*, Sitzungsberichte der Heidelberger Akademie, 1923, No. 3.

‡ S. MacLane, *The ideal-decomposition of rational primes in terms of absolute values*, Proceedings of the National Academy of Sciences, vol. 21 (1935), pp. 663–667.

§ O. Ore, loc. cit., Theorem 1, p. 99.

(mod q) and hence $aQ=(q, \alpha+a_1)$. Thus $\alpha+a_1$ and, by IIa, $a_2, a_3, \cdots, a_n$ are divisible by Q. Hence

$$b_i = \alpha^{i-1}(\alpha + a_1) + a_2\alpha^{i-2} + a_3\alpha^{i-3} + \cdots + a_i \equiv 0 \pmod{Q}, \qquad (i = 1, 2, \cdots, n-1).$$

Since $b_{n-1}\alpha = a_n$ and $a_n \not\equiv 0 \pmod{q^2}$, we have $b_{n-1}\not\equiv 0 \pmod{Q^2}$. Consequently $f_1(x)$ in (3) satisfies the Eisenstein irreducibility criterion with respect to Q, and G is doubly transitive as before.

Condition IIb gives a prime ideal $Q=(q, \alpha-c)$ in $R(\alpha)$, with $f_1(x)\equiv\phi(x) \pmod{Q}$. But Q is of first degree, so that the residue-class field of integers (mod Q) is identical to the field of integers (mod q), and $\phi(x)$ must thus remain irreducible (mod Q). Hence $f_1(x)$ is irreducible.

From condition IIIa we prove by induction that the group G contains a transposition. If $n=2, f(x)=x^2+a_1x+a_2\equiv x^2 \pmod{p}$, $a_2\not\equiv 0 \pmod{p^2}$, $f(x)$ is irreducible by Eisenstein's criterion and its group contains a transposition interchanging the roots. For $n>2$, let $h(x)$ be the irreducible factor of $f(x)$ divisible by $\psi_1(x)$ (mod p) and let α be a root of $h(x)$. Corresponding to ψ_1 there is a prime ideal $P=(p, \psi_1(\alpha))$ in $R(\alpha)$. The remaining equation $f_1(x)=f(x)/(x-\alpha)$ will have a decomposition

$$f_1(x) \equiv x^2\theta_1(x)\cdot\theta_2(x) \cdots \theta_s(x) \pmod{P},$$

where each $\theta_i(x)$ is an irreducible factor of some $\psi_j(x)$ (mod P). If two θ_i's were congruent mod P, then either $\psi_j(x)$ would have a multiple root (mod P), contrary to the fact that an irreducible polynomial over a finite field never has multiple roots, or else two factors $\psi_j(x)$ and $\psi_k(x)$ would have a root in common (mod P), which is impossible. Hence the $\theta_i(x)$ are distinct and distinct from x, while $b_{n-1}\not\equiv 0 \pmod{P^2}$. Thus $f_1(x)$ satisfies the same conditions with respect to P over $R(\alpha)$ as did $f(x)$ with respect to p over R, and the induction assumption, which holds over any algebraic field, yields the required transposition in G.

The treatment of IIIb is similar. Since $\psi_1(x)$ is of odd degree, the prime ideal $P=(p, \psi_1(\alpha))$ has a residue-class field of odd degree over the field of integers mod p. Hence $\phi(x)$, of even degree, must remain irreducible over such a residue-class field. The irreducible factors of $\psi_i(x)$ (mod P) are factors of an irreducible polynomial over a normal extension field, hence have degrees which are divisors of the odd degree of $\psi_i(x)$. Induction thus applies, and gives, for $n=2$, $f_{n-2}(x)\equiv\phi(x)$, hence irreducible.

This method of constructing equations without affect has the advantage of generality. Theorem 1 is true and the construction can be readily carried out if the a_i are integers of any algebraic field, while p, q, and r are prime ideals in that field. More generally, we can replace the primes by "absolute values." A discrete non-archimedean absolute value* U of a field K is a function such that, for any a in K, $U(a)$ is a rational integer or $+\infty$, with the properties

$$U(ab) = U(a) + U(b); \; U(a+b) \geqq \min\,(Ua, Ub).$$

Since the Eisenstein irreducibility theorem and the Newton polygon construction generalize to such absolute values, we can state the following theorem.

THEOREM 3. *If the polynomial $f(x)$ in* (1) *has coefficients a_i in any field K, if $f(x)$ is separable and if the conditions* I, II, *and* III *of Theorem* 1 *hold when Ua_i (or Va_i, or Wa_i) takes the place of the power to which a_i is divisible by p (or q, or r), then $f(x)$ is without affect over K.*

For example, if $K=R(y_1, \cdots, y_m)$ is the field of rational functions of m variables $y_1, \cdots, y_m$ with rational coefficients, a particular value U can be defined thus: Consider any irreducible polynomial $\phi(y_1, \cdots, y_m)$, set Ug for any polynomial $g(y_1, \cdots, y_m)$ equal to the highest power to which g is divisible by ϕ, and set $U(g/h)=Ug-Uh$ for any rational function g/h. Hence *Theorem* 1 *remains true if the a_i are polynomials in $y_1, \cdots, y_m$, while p, q, and r are three irreducible polynomials in the same variables.*

HARVARD UNIVERSITY

[*] W. Krull, *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, no. 3.