BULLETIN OF THE

AMERICAN MATHEMATICAL SOCIETY.

CRITERIA FOR THE IRREDUCIBILITY OF FUNCTIONS IN A FINITE FIELD.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, September 3, 1906.)

1. THEOREM. *A necessary condition that*

$$f(x) \equiv x^m + c_1 x^{m-1} + \cdots + c_m \tag{1}$$

shall be irreducible in the GF $[p^n]$, $p > 2$, *is that its discriminant* * *be a square or a not-square according as m is odd or even.*

If $f(x) = 0$ is irreducible its roots are $\lambda^{p^{ni}} (i = 0, 1, \cdots, m-1)$. Its discriminant is therefore the square of P, where

$$P = \prod_{i<j}^{i,j=0,1,\ldots,m-1} (\lambda^{p^{ni}} - \lambda^{p^{nj}}) \equiv \Pi f_{i,j}.$$

For $j < m-1$, we have $f_{i,j}^{p^n} = f_{i+1,j+1}$. But $f_{i,m-1}^{p^n} = -f_{0,i+1}$.

Hence

$$P^{p^n} = (-1)^{m-1} P,$$

so that P equals a mark of the $GF[p^n]$, $p > 2$, if and only if m is odd.

Remark. The condition is also sufficient if $m = 2$.

2. LEMMA. *The necessary and sufficient condition that a cubic shall have one and but one root in the* $GF[p^n]$, $p > 2$, *is that its discriminant be a not-square.*

* As in the theory of algebraic equations, it is here convenient to designate as the discriminant the product of the squares of the differences of the roots. Most writers on cognate subjects insert the factor $(-1)^{\frac{1}{2}m(m-1)}$, and some insert also the factor $1/m^m$.

The condition is necessary. For, if the cubic has a linear and an irreducible quadratic factor, its roots are

$$y_1 \equiv y_1^{p^n}, \quad y_2, \quad y_3 \equiv y_2^{p^n} \quad (y_2^{p^{2n}} = y_2).$$

Then its discriminant Δ equals π^2, where

$$\pi = (y_1 - y_2)(y_1 - y_2^{p^n})(y_2 - y_2^{p^n}), \quad \pi^{p^n} = -\pi.$$

Since π is not in the $GF[p^n]$, $p > 2$, Δ is a not-square.

The condition is sufficient. For, if Δ is a not-square, the cubic is reducible (§ 1). But not all three roots lie in the $GF[p^n]$, since Δ would then be a square in the field.

3. THEOREM.* *The necessary and sufficient conditions that*

$$x^3 + \beta x + b = 0 \tag{2}$$

be irreducible in the $GF[p^n]$, $p > 3$, *are the following two:*

(3) $R \equiv -4\beta^3 - 27b^2 = a$ *square* $\neq 0$ *in* $GF[p^n]$, *say* $R = 81\mu^2$;

(4) $\frac{1}{2}(-b + \mu\sqrt{-3}) = a$ *not-cube in the field* $(GF[p^n], \sqrt{-3})$.

We suppose that the necessary condition (3) is satisfied. In (2) set $x = y - \beta/3y$. Then

$$(2y^3 + b)^2 = -R/27 = -3\mu^2. \tag{5}$$

Now -3 is a square or a not-square in the $GF[p^n]$, $p > 3$, according as $(x^3 - 1)/(x - 1) = 0$ is or is not solvable, *i. e.*, according as $p^n - 1$ is or is not divisible by 3.

First, let p^n be of the form $3l + 1$, so that -3 is the square of a mark τ in the $GF[p^n]$. Then (5) gives $y^3 = \frac{1}{2}(-b + \mu\tau)$. If the second member were a cube in the field, (2) would have a root in the field. Hence (4) is a necessary condition for irreducibility. Further, it is a sufficient condition. For, if $\frac{1}{2}(-b + \mu\tau)$ is a not-cube ν, $y^3 = \nu$ is irreducible in the $GF[p^n]$. The same is true of (2). Indeed, if it had a root x in the field, then y would satisfy the quadratic $x = y - \beta y^2/3\nu$, in contradiction to the irreducibility of $y^3 = \nu$.

* From §§ 2, 3, we deduce complete criteria for the nature of the roots of a cubic.

Next, let p^n be of the form $3l + 2$, so that $\tau^2 = -3$ defines the $GF[p^{2n}]$. If

$$\tfrac{1}{2}(-b + \mu\tau) = (r + s\tau)^3, \quad r \text{ and } s \text{ in the } GF[p^n],$$

then

$$\tfrac{1}{2}(-b - \mu\tau) = (r - s\tau)^3.$$

The product of the left members equals $-\beta^3/27$. Hence

$$y = r + s\tau, \quad -\beta/3y = r - s\tau, \quad x = 2r,$$

so that (2) would be reducible. To show that (4) is also a sufficient condition, let $\frac{1}{2}(-b + \mu\tau)$ be a not-cube ν in the $GF[p^{2n}]$. Then if (2) had a root x in the $GF[p^{2n}]$, y would satisfy two equations with coefficients in this field, $x = y - \beta y^2/3\nu$, $y^3 = \nu$, whereas the latter is irreducible.

4. When $p^n = 3l + 2$, there are $\frac{2}{3}(p^{2n} - 1)$ not-cubes * ν in the $GF[p^{2n}]$. For a given ν, marks b and β of the $GF[p^n]$ are uniquely determined by the condition $\frac{1}{2}(-b + \mu\sqrt{-3}) = \nu$, viz.,

$$-b = \nu + \nu^{p^n}, \quad -\beta^3/27 = \nu^{p^n+1}.$$

By the latter, $\beta = -3f\nu^{l+1}$, where $f^3 = 1$. Then $\beta^{p^n} = \beta$ if and only if

$$f\nu^{\frac{1}{3}(p^{2n}-1)} = 1, \quad \beta = -3\nu^{-\frac{1}{3}(p^n-2)(p^n+1)}.$$

The values of b and β are unaltered by the replacement of ν by either ν or ν^{p^n}, but at least one is altered by any new replacement. *When* $p^n = 3l + 2$, *there exist exactly* $\frac{1}{3}(p^{2n} - 1)$ *irreducible cubics* (2) *in the* $GF[p^n]$; *these are given by*

$$(6) \quad x^3 - 3x\nu^{-\frac{1}{3}(p^n-2)(p^n+1)} - \nu - \nu^{p^n} = 0 \quad (\nu \text{ a not-cube in } GF[p^{2n}]).$$

5. When $p^n = 3l + 1$, (4) requires that

$$\tfrac{1}{2}(-b + \mu\sqrt{-3}) = \nu, \quad \tfrac{1}{2}(b + \mu\sqrt{-3}) = \beta^3/27\nu \quad (\nu \text{ a not-cube}),$$

since the product of the first members is $\beta^3/27$. Hence

$$b = \beta^3/27\nu - \nu, \quad \mu\sqrt{-3} = \beta^3/27\nu + \nu.$$

* The powers of a primitive root with exponents prime to 3.

For these values, (3) is satisfied. Now b is unaltered by the replacement of ν by either ν or $-\beta^3/27\nu$, but is altered by any new replacement. Separating the cases $\beta \neq 0$, $\beta = 0$, we obtain

$$\tfrac{1}{2}\cdot\tfrac{2}{3}(p^n-1)(p^n-1)+\tfrac{2}{3}(p^n-1)\equiv\tfrac{1}{3}(p^{2n}-1)$$

sets ν, β giving distinct sets b, β. *When* $p^n = 3l+1$, *there exist exactly* $\frac{1}{3}(p^{2n}-1)$ *irreducible cubics* (2) *in the* $GF[p^n]$; *these are given by*

$$(7)\qquad x^3+\beta x+\beta^3/27\nu-\nu=0 \qquad (\beta \textit{ arbitrary, } \nu \textit{ not-cube}).$$

6. We may otherwise determine the number of irreducible cubics in the $GF[p^n]$. We enumerate the reducible cubics (2).

First, let there be three linear factors $x-f_j$, where $f_1+f_2+f_3=0$. Consider in turn the cases: (*i*) every $f_j=0$; (*ii*) a single $f_j=0$; (*iii*) each $f_j\neq 0$, two equal; (*iv*) each $f_j\neq 0$, all distinct. For the first three cases, the number of cubics is

$$1+\tfrac{1}{2}(p^n-1)+(p^n-1) \text{ if } p>2;\ 1+(p^n-1)+0 \text{ if } p=2.$$

For case (*iv*) it suffices to take as f_1 any mark $\neq 0$, for f_2 any mark distinct from $0, f_1, -f_1, -2f_1, -\frac{1}{2}f_1$, the last three not occurring if $p=2$, and the last two being superfluous if $p=3$. The number of cubics for case (*iv*) is thus

$$\tfrac{1}{6}(p^n-1)(p^n-5) \text{ if } p>3,\quad \tfrac{1}{6}(p^n-1)(p^n-3) \text{ if } p=3,$$
$$\tfrac{1}{6}(p^n-1)(p^n-2) \text{ if } p=2.$$

The number of cubics for cases (*i*)–(*iv*) is therefore

$$1+\tfrac{1}{6}(p^n-1)(p^n+4) \text{ if } p\neq 3,\quad 1+\tfrac{1}{6}(p^n-1)(p^n+6) \text{ if } p=3.$$

Finally, let the function be $(x-f)(x^2+fx+g)$, where the last factor is irreducible. The number of these functions is $\frac{1}{2}p^n(p^n-1)$, since, of the reducible quadratics, p^n have equal roots and $\frac{1}{2}p^n(p^n-1)$ have distinct roots.

Hence the total number of reducible cubics (2) is

$$\tfrac{1}{3}(2p^{2n}+1) \text{ if } p\neq 3;\quad \tfrac{1}{3}(2p^{2n}+p^n) \text{ if } p=3.$$

But the total number of cubics (2) is p^{2n}. *Hence the number of irreducible functions* $x^3+\beta x+b$ *in the* $GF[p^n]$ *is* $\frac{1}{3}(p^{2n}-1)$ *if* $p\neq 3$, *and* $\frac{1}{3}(3^{2n}-3^n)$ *if* $p=3$.

7. It remains to exhibit the $\frac{1}{3}(3^{2n} - 3^n)$ irreducible cubics (2) in the $GF[3^n]$. It is known * that

$$x^p - x/\lambda^{p-1} - \beta/\lambda^p \tag{8}$$

is irreducible in the $GF[p^n]$ if, and only if,

$$\beta^{p^{n-1}} + \beta^{p^{n-2}} + \cdots + \beta^p + \beta \neq 0. \tag{9}$$

Now if $\lambda^{p-1} = \lambda_1^{p-1}$, $\beta/\lambda^p = \beta_1\lambda_1^p$, then $\lambda_1 = \epsilon\lambda$, $\beta_1 = \epsilon\beta$, where $\epsilon^{p-1} = 1$. But if β satisfies condition (9), then also $\epsilon\beta$ does. Hence the number of distinct irreducible functions (8) is

$$(p^n - 1)(p^n - p^{n-1}) \div (p - 1) \equiv p^{2n-1} - p^{n-1}.$$

Hence for $p = 3$ every irreducible cubic (2) is given by (8), (9).

8. Consider next the quartic

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{10}$$

Its discriminant equals that of the resolvent cubic

$$y^3 - by^2 + (ac - 4d)y + 4bd - a^2d - c^2 = 0. \tag{11}$$

When (10) is irreducible in the $GF[p^n]$, its discriminant is a not-square (§1), so that (11) is reducible. To verify this result, let

$$\lambda, \quad \lambda^{p^n}, \quad \lambda^{p^{2n}}, \quad \lambda^{p^{3n}} \qquad (\lambda^{p^{4n}} = \lambda)$$

be the roots of (10). Then (11) has the roots

$$y_1 = \lambda^{p^{2n}+1} + \lambda^{p^{3n}+p^n}, \; y_2 = \lambda^{p^n+1} + \lambda^{p^{3n}+p^{2n}}, \; y_3 = \lambda^{p^{3n}+1} + \lambda^{p^{2n}+p^n}.$$

Hence $y_1^{p^n} = y_1$, $y_2^{p^n} = y_3$, $y_3^{p^n} = y_2$. But $y_2 \neq y_3$. *Hence when* (10) *is irreducible in the* $GF[p^n]$, *its resolvent cubic has a single root in the field.*

Now (11) may be written in the form

$$(\tfrac{1}{4}y^2 - d)(a^2 - 4b + 4y) = (\tfrac{1}{2}ay - c)^2. \tag{11'}$$

But $a^2 - 4b + 4y_1 = t^2$, where

$$t = \lambda + \lambda^{p^{2n}} - \lambda^{p^n} - \lambda^{p^{3n}}, \quad t^{p^n} = -t.$$

Hence t is not in the $GF[p^n]$, $p > 2$, unless $t = 0$.

* Dickson, Linear Groups, p. 29.

9. We first dispose of the special case $t = 0$. Then, by (11′),

$$a^2 - 4b + 4y_1 = 0, \quad \tfrac{1}{2}ay_1 = c.$$

Eliminating y_1, we get

$$c = \tfrac{1}{2}ab - \tfrac{1}{8}a^3. \tag{12}$$

Then the quartic (10) may be written in the form

$$(x^2 + \tfrac{1}{2}ax + \tfrac{1}{2}b - \tfrac{1}{8}a^2)^2 = k, \quad k \equiv (\tfrac{1}{2}b - \tfrac{1}{8}a^2)^2 - d. \tag{13}$$

Then k must be a not-square; otherwise, the quartic would have two quadratic factors with coefficients in the $GF[p^n]$.

Suppose that this condition on k is satisfied. In view of (13), the quartic has no root in the $GF[p^n]$. It remains to find the further conditions in order that (10) shall not be the product of two quadratic factors in the field. Such factors, when existing, must be of the form

$$x^2 + (\tfrac{1}{2}a + r)x + s, \quad x^2 + (\tfrac{1}{2}a - r)x + ds^{-1},$$

where

$$s + ds^{-1} + \tfrac{1}{4}a^2 - r^2 = b, \quad s(\tfrac{1}{2}a - r) + ds^{-1}(\tfrac{1}{2}a + r) = c. \tag{14}$$

Multiplying the first by $\frac{1}{2}a$ and subtracting the result from the second, we obtain, in view of (12),

$$r(ds^{-1} - s + \tfrac{1}{2}ar) = 0. \tag{15}$$

If $r = 0$, (14_1) becomes $(2s + \frac{1}{4}a^2 - b)^2 = 4k$. Hence $r \neq 0$. If $a = 0$, then $s^2 = d$. If d is a square, (14_1) is satisfied when r^2 equals $\pm 2\sqrt{d} - b$; but one of these values is a square, since their product equals the not-square $4k$. The result for this case is stated in the corollary below. Let next $a \neq 0$. If we eliminate r between (15) and (14_1), we obtain after simple modifications

$$\left\{\frac{2}{a}\left(s + \frac{d}{s}\right) - \frac{a}{4}\right\}^2 = w, \qquad w \equiv \frac{5}{16}a^2 - b + 16d/a^2.$$

There exist solutions s in the $GF[p^n]$ if and only if w is a square. In fact, when w is a square, s lies in the field if

$$(\tfrac{1}{8}a^2 \pm \tfrac{1}{2}aw^{\frac{1}{2}})^2 - 4d$$

is a square. But the product of these two expressions is seen to equal the not-square $\frac{1}{4}a^4k$, so that one is a square.

THEOREM. *If the coefficients of the quartic* (10) *satisfy* (12), *it is irreducible in the* $GF[p^n]$, $p > 2$, *if and only if* $(\frac{1}{2}b - \frac{1}{8}a^2)^2 - d$ *and* $\frac{5}{16}a^4 - a^2b + 16d$ *are not-squares.*

Corollary. *In the* $GF[p^n]$, $p > 2$, $x^4 + bx^2 + d$ *is irreducible if and only if* $b^2 - 4d$ *and* d *are not-squares.*

10. THEOREM. *The necessary and sufficient conditions that a quartic* (10), *not satisfying* (12), *be irreducible in the* $GF[p^n]$, $p > 2$, *are that the resolvent cubic shall have* one and but one root* y_1 *in the* $GF[p^n]$ *and that* $a^2 - 4b + 4y_1$ *shall be a not-square.*

These conditions are necessary by § 8 since now $t \neq 0$.

It remains to prove that these conditions are sufficient. Since there are three ways of separating the four roots into pairs, there are exactly three sets of two quadratic factors of (10), viz.,

$$x^2 + \tfrac{1}{2}(a \mp \tfrac{1}{2}t_i)x + \tfrac{1}{2}y_i \mp (\tfrac{1}{2}ay_i - c)/t_i = 0 \quad (t_i^2 = y_i).$$

Note that under the assumptions each $t_i \neq 0$. If a pair of factors have as coefficients marks of the $GF[p^n]$, then y_i and t_i belong to the field. But y_2, y_3 and t_1 are not in the $GF[p^n]$. Hence there is no decomposition into quadratic factors in the field. Finally, we show that there is no linear factor. The quartic may be written in the form

$$X^2 = (a^2 - 4b + 4y_1)Z^2, \quad X \equiv x^2 + \tfrac{1}{2}ax + \tfrac{1}{2}y_1,$$

$$Y \equiv \tfrac{1}{2}x + \frac{\frac{1}{2}ay_1 - c}{a^2 - 4b + 4y_1}.$$

If the quartic has a root x in the field, then $X = Z = 0$. To prove that this is impossible it suffices to set $a = 0$, as may be accomplished by a transformation of the quartic. Then

$$x^2 + \tfrac{1}{2}y_1 = 0, \quad \tfrac{1}{2}x - c/(4y_1 - 4b) = 0$$

require that

$$y_1^3 - 2by_1^2 + b^2y_1 + \tfrac{1}{2}c^2 = 0. \tag{16}$$

* We may replace this condition by the condition that Δ shall be a not-square (§ 2).

On eliminating first y_1^3 and then c^2 between (16) and (11), and in the latter case removing the factor $y_1 - b \neq 0$, we get

$$(17) \quad by_1^2 - b^2y_1 - 4dy_1 + 4bd - \tfrac{3}{2}c^2 = 0, \quad 3y_1^2 - 2by_1 - 4d = 0.$$

But the Sylvester eliminant of these is found to equal $-\frac{3}{4}\Delta$, where Δ is the discriminant of (11) for $a = 0$. Hence the case $p \neq 3$ is excluded. For $p = 3$, $by_1 = d \neq 0$; but for this value of y_1 (11) becomes $\Delta = 0$. Hence in every case the conditions are sufficient to make the quartic irreducible.

UNIVERSITY OF CHICAGO,
June, 1906.

ON THE THEORY OF EQUATIONS IN A MODULAR FIELD.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, September 3, 1906.)

1. The object of this note is to point out that the Galois theory of algebraic equations may be extended to equations in a field F having a modulus p. For a finite field the theory is so obvious that this case furnishes a simple, but characteristic, example of the Galois theory.

2. Let the domain of rationality be the $GF[p^n]$. Consider an equation $f(x) = 0$ with coefficients in this field and having distinct roots $x_1, \cdots, x_m$. By a Galois resolvent of $f(x) = 0$ will be meant an equation $\phi(V) = 0$, irreducible in the $GF[p^n]$, with a root V which is a rational function of $x_1, \cdots, x_m$, and such that each x_i is a rational function of V with coefficients in the field. Let $m_1, m_2, \cdots$ be the distinct degrees of the irreducible factors of $f(x)$ in the $GF[p^n]$, and let l be the least common multiple of $m_1, m_2, \cdots$. Then the smallest field which contains all the roots x_i of $f(x) = 0$ is the $GF[p^{nl}]$. Any primitive root of the latter may be taken as the desired function V. In fact the power $(p^{nl} - 1)/(p^{nm_i} - 1)$ of V is a primitive root ρ_i of the $GF[p^{nm_i}]$, so that the x's are powers of $\rho_1, \rho_2, \cdots$ and hence of V. Further, V is a rational function of the ρ's and hence of the x's. Indeed, if m_1 and m_2 have the greatest common divisor g and the least common multiple λ, an