On the Decomposition of Prime Numbers in a Biquadratic Number-Field.

By Jacob Westlund.

Let

$$x^4 + ax^2 + bx + c = 0$$

be an irreducible equation with integral co-efficients, whose discriminant $\triangle$ we suppose to be a prime number. Denote the roots of this equation by $\theta, \theta', \theta'', \theta'''$, and let us consider the number-field $k(\theta)$, generated by θ. Then since the fundamental number of $k(\theta)$ enters as a factor in the discriminant of every algebraic integer in $k(\theta)$, it follows that $\triangle$ is the fundamental number of $k(\theta)$ and

$$1, \theta, \theta^2, \theta^3$$

form an integral basis, i. e., every algebraic integer α in $k(\theta)$ can be written

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$$

where a_0, a_1, a_2, a_3 are rational integers.

The decomposition of any rational prime p into its prime ideal factors is effected by means of the following theorem: If

$$F(x) = x^4 + ax^2 + bx + c$$

be resolved into its prime factors with respect to the modulus p and we have

$$F(x) \equiv \left\{ P_1(x) \right\}^{e_1} \left\{ P_2(x) \right\}^{e_2} \ldots\ldots \pmod{p}$$

where $P_1(x), P_2(x) \ldots$ are different prime functions with respect to p, of degrees $f_1, f_2, \ldots$ respectively, then

$$(p) = \left[p,\ P_1(\theta) \right]^{e_1} \left[p,\ P_2(\theta) \right]^{e_2} \ldots\ldots$$

where $\left[p,\ P_1(\theta) \right]$, $\left[p,\ P_2(\theta) \right]$ ..... are different prime ideals of degrees $f_1, f_2, \ldots$ respectively. (1)

In applying this theorem to the factorization of p we have two cases to consider, 1st when $p = \triangle$ and 2nd when $p \neq \triangle$.

Case I. $p = \triangle$.

Suppose

$$(p) = A_1^{e_1} A_2^{e_2} A_3^{e_3} A_4^{e_4}$$

where $A_1, A_2 \ldots$ are different prime ideals of degrees $f_1, f_2, \ldots$, respectively. Then, since the fundamental number of $k(\theta)$ is divisible by $p^{f_1(e_1-1)+f_2(e_2-1)+\cdots}$ (1), we have

$$f_1(e_1 - 1) + f_2(e_2 - 1) + f_3(e_3 - 1) + f_4(e_4 - 1) = 1,$$

(1) Hilbert: "Bericht über die Theorie der Algebraischen Zahlkörper," Jahresbericht der Deutschen Mathematiker-Vereinigung (1894-95), pp. 198, 202.

and also

$$f_1^{e_1} + f_2^{e_2} + f_3^{e_3} + f_4^{e_4} = 4.$$

From these two relations we see, remembering that $\triangle$ is divisible by the square of a prime ideal [2], that the required factorization of p is either

$$(p) = A_1^2 . A_2 . A_3$$

where A_1, A_2, A_3 are prime ideals of first degree, or

$$(p) = A_1^2 A_2$$

where A_1 is of first degree and A_2 of second degree.

Hence the factors of F(x) are either

$$F(x) \equiv \left\{ P_1(x) \right\}^2 P_2(x) \,.\, P_3(x) \qquad (\text{mod. } p),$$

where $P_1(x)$, $P_2(x)$, $P_3(x)$ are prime functions of first degree, or

$$F(x) \equiv \left\{ P_1(x) \right\}^2 P_2(x)$$

where $P_1(x)$ is of first degree and $P_2(x)$ of second degree.

In order to find the prime ideal factors of p we have thus to resolve F(x) into its prime factors with respect to the modulus p. To do this we set

$$X^4 + ax^2 + bx + c \equiv (x + l)^2 (x^2 + mx + n) \quad (\text{mod. } p)$$
$$\equiv x^4 + (m + 2l) x^3 + (n + l^2 + 2ml) x^2 + (ml^2 + 2ln) x + nl^2. \quad (\text{mod. } p.)$$

Hence, for determining l, m, n we have the congruences

$$\left.\begin{array}{l} m + 2l \equiv o \\ n + 2ml + l^2 \equiv a \\ ml^2 + 2ln \equiv b \\ nl^2 \equiv c \end{array}\right\} (\text{mod. } p).$$

Eliminating m and n, we get

$$\left.\begin{array}{l} 4l^3 + 2la \equiv b \\ 3l^4 + al_2 \equiv c \end{array}\right\} (\text{mod. } p),$$

which give

$$2al^2 \equiv 3bl - 4c \quad (\text{mod. } p).$$

Having thus obtained the values of l, m, and n, we set

$$X^2 + mx + n \equiv (x + r)(x + s) \quad (\text{mod. } p)$$
$$\equiv X^2 + (r + s) x + rs. \quad (\text{mod. } p).$$

Hence,

$$\left.\begin{array}{l} r + s \equiv m \\ rs \equiv n \end{array}\right\} (\text{mod. } p).$$

or

$$(r - s)^2 \equiv -4 (a + 2l^2) \quad (\text{mod. } p).$$

(1) Hilbert, p. 201. (2) Hilbert, p. 195.

1. If $\left(\frac{-(a+2l^2)}{p}\right) = -1$, then x^2+mx+n is irreducible and we have

$$F(x) \equiv (x+1)^2 (x^2+mx+n) \pmod{p}$$

and hence

$$(p) = (p, \Theta+1)^2 (p, \Theta^2+m\Theta+n).$$

2. If $\left(\frac{-(a+2l^2)}{p}\right) = +1$, then let $r-s=k$ be a solution of $(r-s)^2 \equiv -4(a+2l^2) \pmod{p}$ and we get r and s from the congruences

$$\left.\begin{array}{l} r+s \equiv m \\ r-s \equiv k \end{array}\right\} \pmod{p}.$$

We have then

$$F(x) \equiv (x+1)^2 (x+r)(x+s) \pmod{p}$$

and hence

$$(p) = (p, \Theta+1)^2 (p, \Theta+r)(p, \Theta+s).$$

Case II. $p \pm \triangle$.

In this case we have the two relations

$$f_1(e_1-1) + f_2(e_2-1) + f_3(e_3-1) + f_4(e_4-1) = 0.$$
$$f_1e_1 + f_2e_2 + f_3e_3 + f_4e_4 = 4.$$

Now since $\triangle$ is the only prime which is divisible by the square of a prime ideal, the relations given above show that p can be factored in one of the following ways:

1. $(p) = A_1 \cdot A_2 \cdot A_3 \cdot A_4$ where A_1, A_2, A_3, A_4 are all of 1st degree.
2. $(p) = A_1 \cdot A_2 \cdot A_3$ where A_1 is of 2d degree and A_2, A_3 of 1st degree.
3. $(p) = A_1 \cdot A_2$ where A_1 and A_2 are both of 2d degree.
4. $(p) = A_1 \cdot A_2$ where A_1 is of 1st degree and A_2 of 3d degree.
5. $(p) = A_1$ where A_1 is of 4th degree, in which case (p) is a prime ideal.

Hence F(x) can be factored in one of the following ways:

1. $F(x) \equiv P_1(x) \cdot P_2(x) \cdot P_3(x) \cdot P_4(x) \pmod{p}$.
2. $F(x) \equiv P_1(x) \cdot P_2(x) \cdot P_3(x) \pmod{p}$.
3. $F(x) \equiv P_1(x) \cdot P_2(x) \pmod{p}$.
4. $F(x) \equiv P_1(x) \cdot P_2(x) \pmod{p}$.
5. $F(x) \equiv P_1(x) \pmod{p}$.

where $P_i(x)$ is a prime function of the same degree as the corresponding A.

In order to decompose $F(x)$ into its prime factors with respect to the modulus p we set

$$x^4 + ax^2 + bx + c \equiv (x + l)\ (x^3 - lx^2 + mx + n) \pmod{p}.$$
$$\equiv x^4 + (m - l^2)\, x^2 + (n + lm)\, x + ln \pmod{p}$$

hence,

$$\left.\begin{array}{l} m - l^2 \equiv a \\ n + lm \equiv b \\ ln \equiv c \end{array}\right\} \pmod{p}.$$

from which we get

(1) $l^4 + al^2 - bl \equiv -c. \quad (\text{mod. } p).$

A) If (1) has one solution only, then the prime factors of $F(x)$ are $(x+l)$ and $(x^3 - lx^2 + mx + n)$ and the required factorization of p is

$$(p) = (p, \theta + l)\ (p, \theta^3 - l\theta^2 + m\theta + n).$$

B) If (1) has two solutions l and l'. Then $F(x)$ contains two factors of 1st degree and one of 2d degree and we have

$$F(x) \equiv (x + l)\ (x + l')\ (x^2 + sx + t) \quad (\text{mod. } p).$$

where

$$\left.\begin{array}{l} s \equiv -(l + l') \\ t \equiv a - l^2 - l'^2 - ll' \end{array}\right\} (\text{mod. } p).$$

and hence,

$$(p) = (p, \theta + l)\ (p, \theta + l')\ (p, \theta^2 + s\theta + t).$$

C) If (1) has three solutions in which case it evidently must have four solutions l, l' l'' l''', then

$$F(x) \equiv (x + l)\ (x + l')\ (x + l'')\ (x + l''') \quad (\text{mod. } p).$$

and hence,

$$(p) = (p, \theta + l)\ (p, \theta + l')\ (p, \theta + l'')\ (p, \theta + l''').$$

D) If (1) has no solution, $F(x)$ has no factors of 1st degree. Then we set

$$F(x) \equiv (x^2 + mx + n)\ (x^2 - mx + n') \qquad (\text{mod. } p).$$
$$\equiv x^4 + (n + n' - m^2)\, x^2 + m\, (n' - n)\, x + nn' \quad (\text{mod. } p).$$

Hence,

$$(2) \qquad \left.\begin{array}{l} n + n' - m^2 \equiv a \\ m(n' - n) \equiv b \\ nn' \equiv c \end{array}\right\} (\text{mod. } p).$$

If the system (2) is soluble we have

$$F(x) \equiv x^2 + mx + n)\ (x^2 - mx + n') \quad (\text{mod. } p).$$

and hence,

$$(p) = (p,\ \theta^2 + m\theta + n)\ (p,\ \theta^2 - m\theta + n').$$

If (2) is insoluble, $F(x)$ is irreducible and hence (p) is a prime ideal.

As an application we give a table of the prime ideal factors of certain rational primes in the number-field generated by a root θ of the equation

$$x^4 + x + 1 = 0.$$

Here $\triangle = 229$ and we get

$$(229) = (229,\ \theta - 75)^2\ (229,\ \theta^2 - 79\theta - 71)$$
$$(2) = (2)$$
$$(3) = (3,\ \theta + 2)\ (3,\ \theta^3 + \theta^2 + \theta + 2)$$
$$(5) = (5,\ \theta + 2)\ (5,\ \theta^3 + 3\theta^2 + 4\theta + 3)$$
$$(7) = (7)$$
$$(11) = (11,\ \theta + 4)\ (11,\ \theta^3 - 4\theta^2 + 16\theta + 3)$$
$$(13) = (13)$$
$$(17) = (17,\ \theta - 3)\ (17,\ \theta^3 + 3\theta^2 - 8\theta - 6)$$
$$(19) = (19,\ \theta - 2)\ (19,\ \theta^3 + 2\theta^2 + 4\theta + 9)$$
$$(23) = (23,\ \theta + 4)\ (23,\ \theta + 5)\ (23,\ \theta^2 - 9\theta - 8).$$

Dissociation-Potentials of Neutral Solutions of Lead Nitrate with Lead Peroxide Electrodes.

[**Abstract**.]

By Arthur Kendrick.

To determine if in such solutions and with lead peroxide electrodes electrolytic action takes place at voltages lower than that required for the separation of lead and lead peroxide with platinum electrodes, the method developed by Nernst[1] and Le Blanc[2] was made use of.

Two platinum wires coated with a thick, firm crust of lead peroxide were first used as electrodes. The current-potential curves obtained showed sharp bends at about 0.4 volt. To determine at which electrode the action at this voltage took place an electrode was made of a platinum wire projecting 1mm from a sealed glass tube. This point was coated with the lead peroxide before use each time. The other electrode con-

1. W. Nernst, Bericht. d. deutschen ch. Gesel. 30, p. 1547, 1897.
   L. Glaser, Zeit. für Electrochemie, 4, p. 355, 1898.
   E. Bose, Zeit. für Electrochemie, 5, p. 153, 1899.
2. LeBlanc, Zeit. für ph. Chemie, 12, p. 333, 1892.