REMARK ON A CHARACTERIZATION OF CERTAIN RING CLASS FIELDS BY THEIR ABSOLUTE GALOIS GROUP

CHR. U. JENSEN

Let $j(\omega)$ denote the absolute invariant of the modular group, well known from the theory of elliptic modular functions, usually defined by

$$j(\omega) = 1728\frac{g_2(\omega)^3}{\Delta(\omega)} \qquad I\omega > 0,$$

where $\Delta(\omega)$ stands for the discriminant of the complex lattice generated by 1 and ω and $g_2(\omega)$ is the Weierstrass invariant of this lattice.

If $\Omega = \dot{Q}(\sqrt{-D})$ is an imaginary quadratic number field, it is well known from the theory of class fields with complex multiplication that the "singular values" $j(\alpha)$, where $\alpha \in \Omega$, $I\alpha > 0$, generate algebraic number fields which are abelian over Ω, namely the so-called ring class fields. Detailed references for the literature on the theory of ring class fields may be found in the report of Deuring [1].

In the rather extensive theory of ring class fields it is shown that $\Omega(j(\alpha))/\dot{Q}$ is a normal extension with its Galois group $\mathfrak{G}$ being an extension of the abelian Galois group $\mathfrak{A}$ of $\Omega(j(\alpha))/\Omega$, completely determined by the relations

$$\tau^2 = 1; \qquad \tau\sigma\tau = \sigma^{-1} \quad \text{for all } \sigma \in \mathfrak{A}, \tag{1}$$

where τ is the automorphism sending every number into its complex conjugate.

For sake of brevity we denote $\mathfrak{G}$ by $\mathfrak{G} = \{\tau, \mathfrak{A}\}$.

It is the purpose of this note to give a simple proof for an inversion of the above theorem for which the author has not been able to find any reference. The result concerns the case where the order of the abelian group $\mathfrak{A}$ is an odd number. In fact, we are going to state the following.

THEOREM 1. *Let K be a normal extension of the rational number field $\dot{Q}$ containing some imaginary quadratic field Ω. Suppose that the Galois group, $\mathfrak{G}$, is generated by an abelian subgroup $\mathfrak{A}$ and an element τ, subject to the conditions* (1) *so that $\mathfrak{G} = \{\tau, \mathfrak{A}\}$. If the order n of $\mathfrak{A}$ is odd, then K is contained in a ring class field: $K \subseteq \Omega(j(\alpha))$ (with uniquely determined imaginary quadratic Ω). In particular, the assumption on the Galois group is satisfied for any dihedral group D_{2n} with an*

Received by the editors July 16, 1962.

odd n, or more specially, for any nonabelian group $\mathfrak{G}$ of order $2p$ with p being an odd prime.

REMARK. For a more precise result than just K being contained in a ring class field one cannot hope. In fact, the statement is an analogon to the classical Kronecker-Weber Theorem according to which every absolute abelian number field is a subfield of a cyclotomic field.

PROOF. Obviously $\mathfrak{A}$ is a normal subgroup of index 2 in $\mathfrak{G}$. Consequently, the numbers in K left fixed by the automorphisms of $\mathfrak{A}$ form a number field of absolute degree 2. Since the degree of K/Q is $2n$, n being an odd integer, K cannot contain more than one quadratic subfield; hence the imaginary quadratic subfield Ω of K must be the quadratic subfield corresponding to $\mathfrak{A}$.

Now K/Ω is an abelian extension with $\mathfrak{A}$ as its Galois group. Let $\mathfrak{f}$ be the conductor of the corresponding class group $\mathfrak{C}$ in Ω and f the least rational multiple of $\mathfrak{f}$. If $\mathfrak{C}_f$ denotes the group of principal ideals generated by the numbers in the order mod f, the corresponding class field is a ring class field and hence of the form $\Omega(j(\alpha))$ for a suitable $\alpha\in\Omega$, $I\alpha>0$. It suffices to show the inclusion $\mathfrak{C}_f\subseteq\mathfrak{C}$ since this by virtue of the "Anordnungssatz" (see for instance Hasse [2, I, §6, Theorem 10]) implies $K\subseteq\Omega(j(\alpha))$.

In other words, we have to show that any principal ideal (α) with a generator $\alpha\equiv$rational number mod f is contained in $\mathfrak{C}$. Since the ray $\alpha\equiv 1 \bmod f$ surely belongs to $\mathfrak{C}$, it will be sufficient to prove that the set of rational integers prime to f is a subset of $\mathfrak{C}$. According to Artin's reciprocity law this amounts to showing that the Artin symbol $((K/\Omega)/r)=1$ for any rational integer r with $(r,f)=1$.

By the well-known rules valid for the Artin symbol we have for any automorphism σ from $\mathfrak{G}$

$$\left(\frac{\sigma K/\sigma\Omega}{r^\sigma}\right)=\sigma\left(\frac{K/\Omega}{r}\right)\sigma^{-1}.$$

Since $\sigma K=K$, $\sigma\Omega=\Omega$ and $r^\sigma=r$, we have

$$\left(\frac{K/\Omega}{r}\right)=\sigma\left(\frac{K/\Omega}{r}\right)\sigma^{-1}\qquad\text{for all }\sigma\in\mathfrak{G},$$

which means that $((K/\Omega)/r)$ is an element of the centre of $\mathfrak{G}$. Now, as the order n of $\mathfrak{A}$ is odd, it is easily verified that $\mathfrak{G}$'s centre consists of the identity only. Hence we have that $((K/\Omega)/r)=1$. Q.E.D.

As an application of the above theorem in elementary number theory we consider the cubic congruence

$$f(x) = x^3 + ax^2 + bx + c \equiv 0 \mod p \tag{2}$$

with integral a, b and c.

If D denotes the discriminant of $f(x)$ and p a prime >3, Skolem (see for instance Holzer [3, §24, Theorem 1]) has shown that $(D/p) = -1$ implies that (2) has exactly one root, while $(D/p)=1$ implies that (2) has either three or no roots.

Concerning the last case, $(D/p)=1$, we prove the following.

THEOREM 2. *Let the discriminant D of $f(x)$ be negative and written in the form $D=-\Delta m^2$, where Δ is a square-free natural number. If p is representable by the form $p=u^2+\Delta^2|D|v^2$ for $\Delta\equiv 1$ or 2 mod 4 and $p=\frac{1}{4}(u^2+\Delta^2|D|v^2)$ for $\Delta\equiv 3$ mod 4, the congruence (2) has three distinct solutions.*

PROOF. Let K denote the splitting field (within the field of complex numbers) of $f(x)$ over Q. If p is a prime with $(D/p)=1$ and p splits totally in K, the congruence $f(x)\equiv 0 \mod p$ has three distinct solutions. Obviously, the imaginary quadratic field $\Omega=Q(\sqrt{D})$ is a subfield of K and since the Galois group of K/Q is the symmetric group S_3 Theorem 1, with $\mathfrak{A}$ being the cyclic subgroup of order 3 (or, alternatively, observing that S_3 is a nonabelian group of order 2.3), shows that K is contained in a ring class field over Ω.

It now remains to be shown that the least rational multiple f of the conductor $\mathfrak{f}_{K/\Omega}$ of the extension K/Ω (i.e., for K's class group in Ω) divides Δm. Noticing that the relative discriminant $D_{K/\Omega}$ for K/Ω necessarily divides D we just have to take into account the relation between $D_{K/\Omega}$ and $\mathfrak{f}_{K/\Omega}$ which for a cyclic extension of degree 3 has the form $D_{K/\Omega}=\mathfrak{f}_{K/\Omega}^2$. This may be inferred from the general conductor-discriminant formula ("Führer-Diskriminantensatz")

$$D_{K/\Omega} = \prod_{\chi} \mathfrak{f}_{K/\Omega}^{\chi},$$

where $\mathfrak{f}_{K/\Omega}^{\chi}$ runs over the conductors of the characters χ of K's class group in Ω, or alternatively, from the more special and not so deep theorem (see Hasse [2, Ia, §9, Theorem 3]) which says that $D_{K/\Omega} = \mathfrak{f}_{K/\Omega}^{p-1}$ for any cyclic extension of prime degree p.

In this way we obtain

$$\mathfrak{f}_{K/\Omega}^2 \,|\, D_{K/\Omega} \,|\, D = -\Delta m^2,$$

which implies $\mathfrak{f}_{K/\Omega} \,|\, \sqrt{(-\Delta)}m$, and this again implies $f|\Delta m$, which completes the proof.

As a special case of Theorem 2 we mention the following

COROLLARY. *A noncubic integer d is a cubic residue for any prime $p \equiv 1 \bmod 3$, whose canonical representation $p = \frac{1}{4}(u^2+27v^2)$ has the congruence property $v \equiv 0 \bmod 3d$.*

In fact, we only have to observe that the discriminant of $f(x) = x^3 - d$ is $-27d^2$ and $\Delta = -3$.

REFERENCES

1. M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykopädie Math. Wiss., Vol. 12, Book 10, Part II, Teubner, Stuttgart, 1958.

2. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. I, Ia, Jber. Deutsch. Math.-Verein. **35–36** (1926–27), 1–55, 233–311.

3. L. Holzer, *Zahlentheorie*. I, Mathematische-Naturwissenschaftliche Bibliothek **13**, Teubner, Leipzig, 1958.

UNIVERSITY OF COPENHAGEN, DENMARK