J. Austral. Math. Soc. (*Series A*) 40 (1986), 276–286

CHINESE REMAINDER THEOREMS AND GALOIS MODULES

NEIL ORMEROD

(Received 17 August, 1984; revised 13 November 1984)

Communicated by G. Brown

Abstract

This paper studies the relationship between a normal algebraic extension L of an algebraic number field K, viewed as a Galois module, and valuations of the field L. In particular, the paper seeks to establish a relationship between Galois submodules of L and certain types of Chinese Remainder Theorems.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 A 55.
Key words and phrases: Galois modules, Chinese Remainder Theorems.

1. Introduction

The purpose of this paper is to consider the possibility of introducing arithmetically defined norms on naturally arising Galois modules. Having introduced such norms, one can ask how independent inequivalent norms are; that is, there arises the question of Chinese Remainder Theorems. As we shall see, the possibility of satisfying some type of Chinese Remainder Theorem is linked to the representation type of the module considered. The bulk of this paper is concerned with basic machinery and results. The final section, however, deals with possible applications of the type of results we are considering.

As a model of much of what follows, consider the following situation. Let L be a finite normal extension of K, a finite algebraic extension of $\mathbb{Q}$, and let $G = G(L/K)$. Then it is well known that L has a normal basis over K, so that, as a KG module, L is the left regular representation. Let us prove this using the Chinese Remaider Theorem for L.

THEOREM 1. *Let L be a finite normal extension of K, with K a finite algebraic extension of $\mathbb{Q}$, and let $G = G(L/K)$. Then as a KG module L is the left regular representation, i.e. L has a normal basis.*

PROOF. By the Chinese Remainder Theorem for L we have

$$K_v \otimes_K L \cong \bigoplus_{w|v} L_w$$

(cf. [2, pages 54 ff]). Since G acts transitively on the right-hand side, we see that the right-hand side forms a system of imprimitivity for the module $K_v \otimes_K L$. Hence the left-hand side is an induced G_w module, where G_w is the decomposition group of L_w. However, by Cebotarev's Theorem [7, page 165], there exist primes v such that, for $w|v$, we have $G_w = 1$ and $L_w = K_v$. But then $K_v \otimes_K L$ is simply the left regular representation of G, and hence so is L.

Although we have had to invoke some rather powerful results to obtain a normal basis theorem, it does point out the rather strong connection between the arithmetic of a field, via the Chinese Remainder Theorem, and its module structure.

2. Norms on Galois modules

Let L be a finite normal extension of a field K, where K is some finite algebraic extension of $\mathbb{Q}$. Let M be some K subspace of L. For w, any finite prime of L, define a norm on M as follows. For $x \in M$, let

$$\|x\|_w = |x|_w^{n_v^{-1}}, \qquad n_v = [L_w : K_v].$$

It is clear that this defines a norm on M, i.e. that

1. $\|x\|_w > 0 \; \forall x \neq 0$,
2. $\|ax\|_w = |a|_v \|x\|_w \; \forall a \in K$, $w|v$, and
3. $\|x + y\|_w \leqslant \|x\|_w + \|y\|_w$, $x, y \in M$.

Of course different w may induce equivalent norms on M, and we write $w_1 \sim w_2$, so that we obtain an equivalence class $W_1 = \{w | w \text{ a prime of } L, w \sim w_1\}$.

The following lemma clarifies the obvious observation that if $w_1|v_1$ and $w_2|v_2$, for v_1, v_2 distinct primes in K, then $w_1 \nsim w_2$.

LEMMA 1. *Let $\| \|_{w_1}, \ldots, \| \|_{w_r}$ be a set of norms, with w_i lying over distinct primes v_i of K. Then for all $a_1, \ldots, a_r \in M$ and $\varepsilon > 0$, there exists $z \in M$ such that*

$$\|z - a_i\|_w < \varepsilon$$

for all $w|v_i$.

https://doi.org/10.1017/S1446788700027257 Published online by Cambridge University Press

PROOF. By the Chinese Remainder Theorem for K, there exist pairs of algebraic integers in $\mathcal{O}_K$, such that, given any $\varepsilon' > 0$, we have

$$X_{1i} + X_{2i} = 1,$$

where $|X_{1i}|_{v_i} < \varepsilon'$, $|X_{2i}|_{v_j} < \varepsilon'$ for all $j \neq i$ (cf. [2, page 48]). Put $z = \sum_{j=1}^{r} X_{2j} a_j$. Then

$$\begin{aligned} \|z - a_i\|_w &= \left\| (X_{2i} - 1)a_i + \sum_{j \neq i} X_{2j} a_j \right\|_w \\ &= \left\| X_{1i} a_i + \sum_{j \neq i} X_{2j} a_j \right\|_w \\ &\leqslant 2^r \max_{j \neq i} \left\{ \|X_{1i} a_i\|_w, \|X_{2j} a_j\|_w \right\} \\ &\leqslant \varepsilon' 2^r \max \left\{ \|a_j\|_w \right\}, \end{aligned}$$

for all $w|v$. However, we can make the right-hand side as small as we please.

Let us further suppose that M is G-invariant, where $G = G(L/K)$. Thus M becomes a KG module. For a fixed prime v of K, G acts transitively on the primes $w|v$ of L, so that G also acts transitively on the equivalence classes W of norms on M. Put $\Gamma_W = \{ g \in G | gW = W \}$. Then Γ_W plays the role of the usual decomposition subgroup $G_w = \{ g \in G | gw = w \}$. The following observations are trivial.

01. G_w is a subgroup of Γ_W if $w \in W$.

02. $|\Gamma_W : G_w|$ is the number of w in a given equivalence class.

03. $|G : \Gamma_W|$ is the number of inequivalent norms on M lying over v.

04. $\Gamma_{gW} = g \Gamma_W g^{-1}$.

Our major aim will be to show how the arithmetic properties of our norms, as given in terms of Chinese Remainder-type Theorems, are related to the representation type of the GK module M.

Notationally I shall pass from equivalence classes W to elements $w \in W$ and vice-versa, whichever seems more natural in a given setting.

3. Chinese Remainder Theorems

I shall say that M satisfies the *Chinese Remainder Theorem* (CRT) if the following holds:

Let $\| \|_{w_1}, \ldots, \| \|_{w_r}$ be inequivalent norms on M. For all $a_1, \ldots, a_r$ in M, and for all $\varepsilon > 0$, there exists $z \in M$ such that $\|z - a_i\|_{w_i} < \varepsilon$, i.e. the image of M under the diagonal mapping of $M \to \oplus_i M_{w_i}$ defined by $z \mapsto (z, \ldots, z)$ is dense, where M_w is the completion of M under the norm $\| \|_w$.

https://doi.org/10.1017/S1446788700027257 Published online by Cambridge University Press

As in Theorem 1, we have the following.

THEOREM 2. *If M is a G-invariant subspace of L and satisfies the CRT, then M is monomial.*

PROOF. Since M satisfies the CRT we have, as in Theorem 1, that

$$K_v \otimes_K M \equiv \bigotimes_{w|v} M_w,$$

where the sum is over all inequivalent norms induced by $w|v$. Thus $K_v \otimes_K M$ is an induced $K_v\Gamma_W$ module. Again by Cebotarev's Theorem there exist primes v such that $K_v = L_w$. However, we clearly have an injection $M_w \to L_w$, so that $\dim M_w = 1$. Thus $K_v \otimes_K M$, and hence M, is monomial.

Thus the CRT is a fairly restrictive condition. Indeed, the following lemma from group theory indicates some further restrictions.

LEMMA 2. *Let H be a normal subgroup of G, and let θ be a character of H. Assume that θ^G is irreducible. Then $\theta^G|_H$ is multiplicity free.*

PROOF. By a standard corollary to Mackay's irreducibility criterion, θ^G is irreducible if and only if θ and θ^x are distinct for all $x \in H$, and θ is irreducible, where $\theta^x(g) = \theta(x^{-1}gx)$ (cf. [6, Proposition 23 and the following corollary, pages 59–60]).

However, we clearly have by the definition of induced representations that $\theta^G|_H = \sum_{x \in G/H} \theta^x$. The lemma then follows immediately.

COROLLARY 1. *Suppose K is a splitting field for the representations of Γ_W, a normal subgroup of G, where if $w \in W$, then $L_w = K_v$. Then M is irreducible and satisfies the CRT if and only if M is one dimensional.*

PROOF. First, it is clear that if M is one dimensional, then it is irreducible and satisfies the CRT. Conversely, by Theorem 2 we have that M is an induced Γ_W module and that $K_v \otimes_K M \cong \oplus_{w|v} M_w$. Fix v such that, if $w|v$, then $K_v = L_w$. Then we also have a decomposition $M = \oplus M_i$ into irreducible $K\Gamma_{W_1}$ modules, by our assumption on K, and this decomposition is unique because of the multiplicity free result in Lemma 2. Thus

$$K_v \otimes_K M \cong \bigoplus K_v \otimes_K M_i \cong \bigoplus_{w|v} M_w.$$

Now consider the projection onto the first component of the extreme right-hand side $\oplus K_v \otimes_K M_i \to M_{w_1}$. This is a homomorphism of $K_v\Gamma_{W_1}$ modules, and hence the kernel is a $K_v\Gamma_{W_1}$ module. By the uniqueness of the left-hand side, some

https://doi.org/10.1017/S1446788700027257 Published online by Cambridge University Press

$K_v \otimes_K M_i$ must be annihilated. But this is impossible since we have natural injections $M_i \to M \to M_w$. Thus we must have $K_v \otimes_K M \cong M_{w_1}$ and by our choice of v, the right-hand side is clearly one-dimensional.

Note that some such condition on K as given in the corollary is necessary. For instance, the first example in Section 5 clearly satisfies the CRT and is irreducible. However, since $\mathbb{Q}$ does not contain the cube roots of unity, K_2 cannot be split into absolutely irreducible submodules over $\mathbb{Q}$ when $\Gamma_w \cong \langle (123) \rangle$.

Let us seek a more general form of Chinese Remainder Theorem. Let W denote an equivalence class of norms on M. Clearly then gW is another equivalence class. For H a subgroup of G, let HW denote the H orbit of W. Then g_1W and g_2W are both in HW if and only if g_1 and g_2 lie in the same (H, Γ_W) double coset. Then M is said to satisfy the *H-Chinese Remainder Theorem* (*H-CRT*) if the following holds:

Let $\| \|_{w_1}, \ldots, \| \|_{w_r}$ be norms which belong to distinct H orbits HW_i. For all $a_1, \ldots, a_r \in M$, and for all $\varepsilon > 0$, there exists $z \in M$ such that $\|z - a_i\|_w < \varepsilon$ for all $w \in HW_i$.

The motivation for considering such a definition is that the primes of the intermediate field F, the fixed field of H, are naturally indexed by double cosets (H, G_w). Notice that if M satisfies the H-CRT, then it also satisfies the H^g-CRT for all $g \in G$. First consider the situation when H is a normal subgroup of G.

THEOREM 3. *Let H be a normal subgroup of G, and suppose that M satisfies the H-CRT. Then M is an induced $H\Gamma_W$ module.*

PROOF. First note that if H is normal, then the double sets (H, Γ_W) correspond to (single) cosets of the subgroup $H\Gamma_W$. Now define a new norm on M by

$$\|x\|_{HW} = \max_{w \in HW} \|x\|_w.$$

Let M_{HW} denote the completion of M in the resulting topology. Then, again by the H-CRT, we have that $K_v \otimes_K M \cong \oplus_i M_{HW_i}$, where the sum runs over all H-orbits of equivalence classes lying over v. Again the right-hand side forms a system of imprimitivity with decomposition group $H\Gamma_W$, so that M is an induced $H\Gamma_W$ module.

Again, as with Theorem 2, the following corollary indicates some of the limits of the theorem.

COROLLARY 2. *Suppose K is a splitting field for the representations of the subgroup $H\Gamma_W$ normal in G. Then M is irreducible and satisfies the H-CRT only if there is one H-orbit of inequivalent norms lying over the prime v of K.*

PROOF. This follows as in Corollary 1.

Now let us turn our attention to the case when H is not normal in G. The above proof breaks down because the relationship $K_v \otimes_K M \cong \oplus_i M_{HW_i}$ no longer gives rise to a system of imprimitivity since g: $M_{HW} \to M_{Hg^{-1}W}$. All we can say is that the right hand terms are H-invariant. If, however, we further assume that $\Gamma_W = 1$, then we have that $HW \cap H^g gW = \varnothing$ unless $g \in H$. With these observations we may prove the following.

THEOREM 4. *Assume that for some w, we have $\Gamma_W = 1$. If M satisfies the H-CRT, then M is an induced H module.*

PROPOSITION. As before we have that $K_v \otimes_K M \cong \oplus_i M_{HW_i}$, as well as $K_v \otimes_K M \cong \oplus_i M_{H^g W_i}$, since M also satisfies the H^g-CRT. Choose v so that $\Gamma_{W_1} = 1$. Now let $G = \cup g_i H$ be a coset decomposition of G, and consider the mapping

$$K_v \otimes_K M \to \bigoplus_{g \in G/H} M_{H^g gW_1}$$

obtained by summing over the projections $K_v \otimes_K M \to M_{H^g gW_1}$. Since $\cup_{g \in G/H} H^g gW_1$ exhausts all divisors of v, the mapping is injective. Moreover, since we can solve for $x \in K_v \otimes_K M$, where

$$x \mapsto (0, \ldots, 0, y, 0, \ldots, 0) \in \bigoplus_{g \in G/H} M_{H^g gW_1},$$

by the corresponding solution

$$x \mapsto (0, \ldots, 0, y, 0, \ldots, 0) \in \bigoplus_i M_{H^g W_i},$$

where the non-zero term occurs in the $W_i = gW_1$ component, we see that the mapping is surjective. Thus we have an isomorphism

$$K_v \otimes_K M \cong \bigoplus_{g \in G/H} M_{H^g gW_1},$$

where, now the right-hand side forms a system of imprimitivity with decomposition group H. Thus M is an induced H module.

4. Converse results

Of course what has been shown in the previous section is of little interest if no modules can be shown to satisfy any type of Chinese Remainder Theorem. Our aim now will be to construct modules which do just that.

https://doi.org/10.1017/S1446788700027257 Published online by Cambridge University Press

Let H be a subgroup of G, with fixed field F. For M' an FH module and any $g \in G$, gM' is an F^gH^g module. Now put $M = \sum_{g \in G/H} gM'$. Then M is clearly a KG module with dimension less than or equal to $[G: H]^2 \dim M'$.

THEOREM 5. *The module M constructed above satisfies the H-CRT for H normal in G.*

PROOF. Let x be in M, say. Then $x = \sum_{g_i \in G/H} g_i x_i$ for some $x_i \in M'$, so that

$$\begin{aligned} \|x\|_w &= \Big\|\sum g_i x_i\Big\|_w \\ &\leqslant 2^m \max_i \|g_i x_i\|_w \quad (\text{where } m = [G: H]) \\ &= 2^m \max_i \|x_i\|_{g_i^{-1}w}. \end{aligned}$$

Thus, given $a_1, \ldots, a_r \in M$ with $a_i = \sum_j g_j a_{ij}$, we have that

$$\|x - a_i\|_{w_i} \leqslant 2^m \max_j \|x_j - a_{ij}\|_{g_j^{-1}w_i}.$$

Thus we need only consider approximations of the type $\|x_j - a_{ij}\|_{g_j^{-1}w_i}$. However, by Lemma 1, if $\{g_j^{-1}w_i\}_{i=1}^r$ lie over distinct primes v' of F, solutions x_j in M' can be found such that

$$(*) \qquad \|x_j - a_{ij}\|_{g_j^{-1}w} < \varepsilon$$

for all $g_j^{-1}w|v'$, if we are given that $g_j^{-1}w_i|v'$. Now if $w_1, \ldots, w_r$ lie in distinct H orbits, so also do $g_j^{-1}w_1, \ldots, g_j^{-1}w_r$, since H is normal, so they lie over distinct primes of v' of F. Thus solutions x_j to $(*)$ exist such that

$$\|x - a_i\|_w \leqslant 2^m \max_j \|x_j - a_{ij}\|_{g_j^{-1}w} \leqslant 2^m \varepsilon$$

for all w in the same H-orbit as w_i.

It is not at all clear how to generalise this to the case where H is not normal. As indicated by the nature of Theorem 4, when H is not normal extra conditions must be applied, and so we would expect the situation to be more complex. Perhaps a different construction is required.

5. Examples

Perhaps it would be wise to conclude with some concrete examples, which hopefully will illustrate some of what is and what is not possible.

EXAMPLE 1. Let $L = \mathbf{Q}(\omega, \sqrt[3]{2})$, where $\omega^3 = 1$, $\omega \neq 1$, and let $K = \mathbf{Q}$, $F = \mathbf{Q}(\omega)$, and $M = \sqrt[3]{2}\,\mathbf{Q}(\omega)$. For simplicity let us consider valuations rather than norms. Let w be a prime of L. For $x \in M$, we have $x = \sqrt[3]{2}\,z$, where $z \in \mathbf{Q}(\omega)$, so that $|x|_w = |\sqrt[3]{2}|_w |z|_w$. Thus all that is important is the restriction of w to F, so that w_1 and w_2 induce equivalent norms if and only if they lie above the same prime v' of F. Moreover, M can be obtained from the type of construction given in Section 4, so that M satisfies the H-CRT, where $H = G(L/F)$. Moreover, for non-ramified primes, $\Gamma_W = H$ if there are two conjugate primes v_1' and v_2' of F which lie over the rational prime p with $w|p$, i.e. when $p \equiv 1 \bmod 3$. Otherwise $\Gamma_W = G$. Thus if $p \equiv 1 \bmod 3$ we have, for inequivalent W_1 and W_2, that $\mathbf{Q}_P \otimes_{\mathbf{Q}} M \cong M_{W_1} \oplus M_{W_2}$. Otherwise, for unramified p, we have $\mathbf{Q}_P \otimes_{\mathbf{Q}} M \cong M_W$.

EXAMPLE 2. Let $L = \mathbf{Q}(\omega, \sqrt[3]{2}, \sqrt{\alpha_1}, \sqrt{\alpha_2})$, and let $K = \mathbf{Q}$, where $\alpha_1 = (1 + \sqrt[3]{2})(1 + \omega\sqrt[3]{2})$ and $\alpha_2 = (1 + \sqrt[3]{2})(1 + \omega^2\sqrt[3]{2})$. Then $G(L/K) \cong S_4$. For convenience put $\alpha_3 = (1 + \omega\sqrt[3]{2})(1 + \omega^2\sqrt[3]{2})$, so that $\sqrt{\alpha_1\alpha_2} = (1 + \sqrt[3]{2})\sqrt{\alpha_3}$, i.e. $\sqrt{\alpha_3} \in L$. Consider the $\mathbf{Q}G$ module $M = \{x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3} | x_i \in \mathbf{Q}\}$. Then the character of M is irreducible and induced from a one-dimensional representation of one of the Sylow-2 subgroups $G^{(2)}$ of S_4. I shall show that M *does not satisfy any H-CRT* for $H = 1$, V_4, or $G^{(2)}$, where $V_4 \cong C_2 \times C_2$ is normal in S_4. If M satisfies the H-CRT for $H = 1$ or V_4, this would mean that M is an induced $H\Gamma_W$ module. This can only be true if $H\Gamma_W = G^{(2)}$ or G. However, if $H\Gamma_W = G^{(2)}$ or G, then M splits into submodules, whose characters, when restricted to $H\Gamma_W$, are irreducible, and the resulting decomposition is multiplicity free. Thus the conditions of Corollaries 1 and 2 are sufficiently fulfilled to say that there can only be one H orbit lying over any rational prime p. Alternatively, if $H = G^{(2)}$, an isomorphism of the type $\mathbf{Q}_p \otimes_{\mathbf{Q}} M \cong \oplus_i M_{HW_i}$ is a decomposition into H invariant subspaces, so once again there can only be one H orbit over any prime p. Let us now calculate a particular Γ_W and show that this is not the case.

For an unramified prime p, the decomposition groups G_w, where $w|p$, are determined by the conjugacy classes of S_4; and by Cebotarev's theorem every conjugacy class occurs. Certainly there exists a prime w in L such that $G_w = \langle\sigma\rangle$, where $\sigma(x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}) = -x_1\sqrt{\alpha_1} - x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}$. In fact $\sigma \in V_4$. Then, since $G_w < \Gamma_W$, we have

$$\begin{aligned}
&\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3} \pm \sigma\left(x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right)\right|_w \\
&\quad \leqslant \max\left\{\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right|_w, \left|\sigma\left(x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right)\right|_w\right\} \\
&\quad = \left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right|_w \leqslant \max\left\{\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2}\right|_w, \left|x_3\sqrt{\alpha_3}\right|_w\right\}.
\end{aligned}$$

But the first term is just $|2(x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2})|_w$ or $|2x_3\sqrt{\alpha_3}|_w$, and $|2|_w = 1$ since 2 is ramified and w is unramified. Thus

$$\max\left\{\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2}\right|, \left|x_3\sqrt{\alpha_3}\right|\right\} \leqslant \left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right| \leqslant \max\left\{\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2}\right|, \left|x_3\sqrt{\alpha_3}\right|\right\},$$

i.e.

$$\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2} + x_3\sqrt{\alpha_3}\right|_w = \max\left\{\left|x_1\sqrt{\alpha_1} + x_2\sqrt{\alpha_2}\right|_w, \left|x_3\sqrt{\alpha_3}\right|_w\right\}.$$

Thus, for $g \in \Gamma_W$, g must preserve the right-hand side.

This can only occur if $g \in G_w$. Thus $\Gamma_W = G_w$. This is incompatible with any of our previous possibilities, and so M cannot satisfy a H-CRT.

It seems in general that it is too much to expect an irreducible module to satisfy some type of Chinese Remainder Theorem. This is not too disappointing when one remembers that irreducible modules are not uniquely given, whereas larger modules, the homogeneous components of a particular irreducible, are. The nicest possible conjecture would then be that if such a module were induced from an H module, then it would satisfy the H-CRT and, moreover, that the two double coset decompositions $\cup Hg_iG_w$ and $\cup Hg_i\Gamma_W$ are identical. This would ensure the automatic fulfillment in Theorem 4, and it would imply that the various decompositions involved are properly indexed by primes from intermediate fields.

6. Applications

I shall consider two types of applications.

(a) Let M be a G-invariant K-subspace of L. Let $\mathcal{O}_M = M \cap \mathcal{O}_L$, and let M^* be the dual of M under the bilinear mapping given by the trace map (M^* is the contragradient of M). Define the discriminant of M to be $\mathcal{D}(M) \equiv [D\mathcal{O}_M : \mathcal{O}_{M^*}]$, where $D\mathcal{O}_M$ is the dual of $\mathcal{O}_M$ (cf. [4, page 11ff]). $\mathcal{D}(M)$ is defined by localisation, i.e.

$$\mathcal{D}(M)\mathcal{O}_{K_v} = \left[\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} D\mathcal{O}_M : \mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_{M^*}\right] = \left[D\left(\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_M\right) : \mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_{M^*}\right].$$

Now if M and M^* satisfy the H-CRT, then

$$\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_M \cong \bigoplus_i \mathcal{O}_{M_{Hw_i}}, \text{ and}$$

$$\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_{M^*} \cong \bigoplus_i \mathcal{O}_{M^*_{Hw_i}},$$

https://doi.org/10.1017/S1446788700027257 Published online by Cambridge University Press

where M_{HW}^{*} is the dual of M_{HW}, so that the local v component of $\mathscr{D}(M)$ has a factorisation into certain "semi-local" components

$$\left[D\mathcal{O}_{M_{HW}} : \mathcal{O}_{M_{HW}^{*}}\right].$$

If, further, the two double coset decompositions $\cup Hg_iG_w$ and $\cup Hg_i\Gamma_W$ are the same, then these "semi-local" components are indexed by primes in the fixed field of H lying over v, e.g. if $M = L$ then $\mathscr{D}(M)$ is the discriminant of the extension of L over K, and this factorisation is well known.

(b) Following Fröhlich [5], note that the Galois modules we have considered have rank 1 over KG. Thus $M = \nu KG$ for some $\nu \in KG$. However, if M satisfies a H-CRT, then $K_v \otimes_K M \cong \oplus M_{HW_i}$. Now in terms of the K_vG module structure of the left-hand side, we see that

$$M_{HW_i} = \nu_{HW_i} K_v\left[Hg_i\Gamma_{W_1}\right]$$

for some fixed Γ_{W_1}, where $\nu_{HW_i} \in K_v[H_{W_i}]$, and where H_{W_i} is the decomposition group of the double coset $Hg_i\Gamma_{W_i}$. Thus

$$K_v \otimes_K M \cong \nu K_vG \cong \oplus \nu_{HW_i} K_v\left[Hg_i\Gamma_{W_1}\right].$$

Therefore, considering ν as a linear map operating on K_vG, we see that $\nu = \oplus \nu_{HW_i}$. Moreover, if we consider $\mathcal{O}_M = M \cap \mathcal{O}_L$ as an $\mathcal{O}_K[G]$ module, we have again, following Frölich, that

$$\mathcal{O}_{K_v} \otimes_{\mathcal{O}_K} \mathcal{O}_M = \nu\beta_v \mathcal{O}_{K_v}[G],$$

where β_v is an invertible element of K_vG. Again, a H-CRT for M would imply that, as linear maps,

$$\nu\beta_v = \oplus \nu_{HW_i}\beta_{HW_i},$$

where

$$\mathcal{O}_{M_{HW_i}} \cong \nu_{HW_i}\beta_{HW_i}\mathcal{O}_{K_v}\left[Hg_i\Gamma_{W_i}\right],$$

and where β_{HW_i} is an invertible element of $K_v[H_{W_i}]$.

For this last process we require that the modules involved satisfy some type of projectivity condition.

References

[1] J. W. S. Cassels and A. Frohlich, *Algebraic number theory* (Academic Press, London, 1967).
[2] J. W. S. Cassels, "Global number fields", in [1], 42–84.
[3] A. Frohlich, *Algebraic number fields* (Academic Press, London, 1977).

[4] A. Frohlich, "Local fields", in [1], 1–41.
[5] A. Frohlich, "Galois module structure", in [4], 133–192.
[6] J.-P. Serre, *Linear representations of finite groups* (GTM Vol. 42, Springer-Verlag, New York, 1977).
[7] J. Tate, "Global class field theory", in [1], 163–203.

Department of Mathematics
University of New South Wales
P. O. Box 1
Kensington, NSW, 2033
Australia