5. Applications

taking χ of order d and using induction: we start with $n = d$ and then successively remove prime factors from d. It remains to show the claim.

By Frobenius reciprocity one has $\langle \chi^G, 1_H^G \rangle_G = \langle \chi, 1_H^G|_D \rangle_D$, which is equal to the multiplicity of χ in the complex representation $\mathbf{C}[G/H]$ of D. The D-set G/H is D-isomorphic to a disjoint union $\coprod_X D/D_X$, where X runs over the D-orbits of G/H, and each D_X is a subgroup of D. The multiplicity of χ in $\mathbf{C}[D/D_X]$ is either 0 or 1, and it is 1 if and only if $D_X \subset \operatorname{Ker}\chi$. Since $N \subset \operatorname{Ker}\chi$, and D/N is cyclic, it follows that $\langle \chi^G, 1_H^G \rangle_G$ is equal to the number of X for which the order of χ divides $[D : ND_X]$. This index is the number of N-orbits of D/D_X, so the claim follows. $\square$

If for a prime number p the roots of unity in L of p-power order generate a cyclic extension of K, then one can show with the lemma (with $D = G$) that the p-part of $w(L^H)$ is a factorizable $\mathbf{Q}^*$-valued function of H. The condition holds for all $p > 2$, so the odd part of $w(L^H)$ is factorizable.

For any prime $\mathfrak{p}$ of K and $d \in \mathbf{Z}$ the number of primes in L^H extending $\mathfrak{p}$ with residue degree d is a $\mathbf{Z}$-valued factorizable function of H. This follows from the lemma if we take D and N to be the decomposition group and the inertia group of $\mathfrak{p}$. If $\mathfrak{p}$ has a cyclic decomposition group D then one can also take $N = 1$, and deduce the same statement with "residue degree" replaced by "local degree".

It follows that the factor $n(H)$ in (4.1) can be replaced by the product of the ramification indices in the extension L/L^H of those primes $\mathfrak{p} \in S(H)$ that extend to a prime of L with non-cyclic decomposition group in L/K. In particular, $n(H)$ is factorizable if S contains no finite ramified primes.

5. Applications

Without giving proofs we indicate some concrete applications of the factor equivalence results given in the last two sections.

(5.1) Cyclic subfield integer index. Let K be a Galois extension of $\mathbf{Q}$ with abelian Galois group G and ring of integers $\mathcal{O}_K$. For a $\mathbf{Z}[G]$-module M let $c_G(M)$ be the index in M of $\sum M^H$, where the sum is taken over those subgroups H of G for which G/H is cyclic. In particular,

$c_G(\mathcal{O}_K)$ is the index in $\mathcal{O}_K$ of the lattice generated by integers in the cyclic subfields of K. An argument of Gillard (see [2, Prop. 1]) implies that $c_G(M)$ only depends on the $\mathbf{Z}[G]$-module structure of M up to factor equivalence. With (3.1) it follows that $c_G(\mathcal{O}_K) = c_G(\mathbf{Z}[G])$. Therefore, one only needs to consider the group ring for the computation of this "cyclic subfield integer index". An explicit formula for $c_G(\mathbf{Z}[G])$ is given in [6]. For instance, if G has type (p,p) for some prime number p then one obtains $c_G(\mathcal{O}_K) = p^{p(p-1)/2}$. In this case one can deduce in particular that every integral basis of $\mathcal{O}_K$ contains a primitive element of K (cf. [5]).

(5.2) CLASS NUMBER INEQUALITIES. Theorem (4.1) gives a relation between the relative position of the groups of units of fields, and their class numbers. Let us consider the fields of degree 8 of Perlis [13]: we take $a \in \mathbf{Z}$ with $|a|$ not a square or twice a square. The fields $K = \mathbf{Q}(\sqrt[8]{a})$ and $K' = \mathbf{Q}(\sqrt[8]{16a})$ are the invariant fields under subgroups H and H' of $G = \mathrm{Gal}(L/\mathbf{Q})$ with $L = \mathbf{Q}(\zeta_8, \sqrt[8]{a})$. The fields K and K' are "arithmetically equivalent", i.e., they have the same zeta-function. One way to see this is by checking that $1_H^G = 1_{H'}^G$. Since $w(K) = w(K')$, Brauer's theorem implies that $hR = h'R'$, where h, h' and R, R' are the class number and regulator of K and K'. There exist integers a for which $h \neq h'$, such as $a = -15$; see [7].

Choose any $\mathbf{Z}[G]$-linear embedding $\varphi\colon X_S \to U_S(L)$, where S is the set of infinite primes of L. Suppose that we also have an injective $\mathbf{Z}[G]$-linear homomorphism $f\colon \mathbf{Z}[G/H'] \to \mathbf{Z}[G/H]$. Applying the functors $\mathrm{Hom}_G(-, X_S)$ and $\mathrm{Hom}_G\big(-, U_S(L)\big)$ to f we get a commutative diagram

$$\begin{array}{ccc} X_S^H & \xrightarrow{f_X} & X_S^{H'} \\ \big\downarrow{\scriptstyle \varphi_1} & & \big\downarrow{\scriptstyle \varphi_2} \\ U_S(K) & \xrightarrow{f_U} & U_S(K') \,. \end{array}$$

With (4.1) and this diagram one sees that the quotient h/h' is given by

$$\frac{h}{h'} = \frac{\#\operatorname{Cok}\varphi_1}{\#\operatorname{Cok}\varphi_2} = \frac{\#\operatorname{Ker} f_U \cdot \#\operatorname{Cok} f_X}{\#\operatorname{Cok} f_U} = \frac{\big[X_S^{H'} : f_X(X_S^H)\big]}{\big[U_S(K') : \mu_{K'} f_U(U_S(K))\big]} \,.$$

Thus, h/h' is equal to the index $i_f = \big[X_S^{H'} : f_X(X_S^H)\big]$ divided by some positive integer. One obtains a bound in the other direction by switching the role of K

and K'. The index i_f is an entirely combinatorial object; it only depends on f and the signature of K. With a judicious choice of the map f as in [13, p. 507] one can get $i_f = 16$ if $a > 0$, and $i_f = 4$ if $a < 0$. One now recovers [13, Th. 8]: we have $h/h' = 2^k$ with $|k| \leq 4$ if $a > 0$ and $|k| \leq 2$ if $a < 0$.

REFERENCES

[1] BRAUER, R. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachr. 4* (1951), 158–174.

[2] BURNS, D. Factorisability, group lattices, and Galois module structure. *J. Algebra 134* (1990), 257–270.

[3] CASSELS, J. W. S. and A. FRÖHLICH (eds.). *Algebraic number theory*. Academic Press, London, 1967.

[4] CASSOU-NOGUÈS, Ph., T. CHINBURG, A. FRÖHLICH and M. J. TAYLOR. L-functions and Galois-modules, pp. 75–139 in: J. Coates and M. J. Taylor (eds.), *L-functions and arithmetic*, Proc. 1989 Durham Symp. London Math. Soc. Lecture Note Ser. 153, Cambridge 1991.

[5] DE SMIT, B. Primitive elements in integral bases. *Acta Arith. 71* (1995), 159–170.

[6] —— On the integers from cyclic subfields in an abelian number field. *Technical Report 96-16*, Universiteit van Amsterdam, 1996.

[7] DE SMIT, B. and R. PERLIS. Zeta functions do not determine class numbers. *Bull. Amer. Math. Soc. (N.S.) 31* (1994), 213–216.

[8] FRÖHLICH, A. L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure). *J. Reine Angew. Math. 397* (1989), 42–99.

[9] —— Module defect and factorizability. *Illinois J. Math. 32* (1988), 407–421.

[10] KANI, E. and M. ROSEN. Idempotent relations and factors of Jacobians. *Math. Ann. 284* (1989), 307–327.

[11] KANI, E. and M. ROSEN. Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties. *J. Number Theory 46* (1994), 230–254.

[12] NELSON, A. M. Monomial representations and Galois module structure. Ph. D. thesis, King's College, University of London, 1979.

[13] PERLIS, R. On the class numbers of arithmetically equivalent fields. *J. Number Theory 10* (1978), 489–509.

[14] RITTER, J. and A. WEISS. Galois action on integral representations. *J. London Math. Soc. (2) 46* (1992), 411–431.

[15] SERRE, J.-P. *Local fields*. Springer-Verlag, New York, 1979.