Linear Algebra and its Applications 438 (2013) 342–347

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

An analogue of Bridges and Mena's theorem for local fields and a local-global principle

Roi Krakovski

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6

ARTICLE INFO

Article history:
Received 2 April 2012
Accepted 31 July 2012
Available online 7 September 2012

Submitted by R.A. Brualdi

Keywords:
p-adic numbers
Character sums
Abelian groups
Minimal polynomials
Local-global principle

ABSTRACT

Let G be an abelian group of finite order n, K a field and $R \subseteq K$ a ring. Let $D = \sum_{g \in G} a_g g \in R[G]$ such that $\chi(D) \in R$ for every character $\chi : G \to K(\xi_n)$ (where $\chi(D) = \sum_{g \in G} a_g \chi(g)$ and ξ_n is a primitive nth root of unity). What does D look like? The case where $K = \mathbb{Q}$ and $R = \mathbb{Z}$ was settled by Bridges and Mena. Here we obtain a complete characterization for the case where K is a finite extension of the field $\mathbb{Q}_p$ and R is its valuation ring under the condition that p does not divide n.

As an application we obtain the following local-global principle for $\mathbb{Z}/q_1q_2\mathbb{Z}$ (where q_1 and q_2 are distinct primes): If $D \in \mathbb{Z}[\mathbb{Z}/q_1q_2\mathbb{Z}]$, then $\chi(D) \in \mathbb{Z}$ for every character $\chi : \mathbb{Z}/q_1q_2\mathbb{Z} \to \mathbb{C}^\times$ if and only if $\psi(D) \in \mathbb{Z}_p$ for every prime p and every character $\psi : \mathbb{Z}/q_1q_2\mathbb{Z} \to \mathbb{Q}_p(\xi_n)$.

1. Introduction

Let G be a finite group. Define an equivalence relation $\sim$ on the elements of G by $x \sim y$ if and only if $\langle x \rangle = \langle y \rangle$ (that is, x and y are equivalent if and only if they generate the exact same subgroup of G). The following was proved by Bridges and Mena [1].

Theorem 1.1. *Let G be a finite abelian group and let $D \in \mathbb{Z}[G]$. Then $\chi(D) \in \mathbb{Z}[G]$ for every character $\chi : G \to \mathbb{C}^\times$ if and only if equivalent elements $x \sim y$ of G have equal coefficients in D (that is, D is constant on equivalence classes of G w.r.t. $\sim$).*

In this paper we obtain an analogue to Theorem 1.1 for local fields and their valuation rings (Theorem 1.2). We then establish a connection between Theorem 1.1 (which concerns with cyclotomic fields) and Theorem 1.2 (which concerns with local fields) for a certain type of cyclic groups.

E-mail address: roikr@cs.bgu.ac.il

0024-3795/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.laa.2012.07.043

We need several definitions in order to present the main results of this paper. Let K be a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. Let $\pi \in K$ be an element of K of maximal absolute value strictly smaller than 1. Let

$$A_K := \{x \in K \mid |x| \leqslant 1\}$$

be the valuation ring of K with maximal ideal

$$M_K := \pi A_K = \{x \in K \mid |x| < 1\}$$

The residue field $k := A_K/M_K$ is finite, hence a finite extension of $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$. If $d = [k : \mathbb{F}_p]$, then $k \cong \mathbb{F}_q$, where $q = |k| = |\mathbb{F}_p|^d = p^d$. (For more details on finite extensions of $\mathbb{Q}_p$ the reader is referred to the excellent book by Robert [2].)

Let $q, n \in \mathbb{N}^*$ such that $(q, n) = 1$ and consider the group $(\mathbb{Z}/n\mathbb{Z})^\times$ (the multiplicative group modulo n). We denote by $\langle q\rangle_n \leqslant (\mathbb{Z}/n\mathbb{Z})^\times$ the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by q and write $\mathrm{ord}_n(q)$ for the order of q in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Let G be an abelian group of order $n \in \mathbb{N}^*$ and let q be a prime power such that $(q, n) = 1$. Define a relation $\sim_q$ on the elements of G by $x \sim_q y$ if and only if $y = x^j$, for some $j \in \langle q\rangle_n$. The relation $\sim_q$ is an equivalence relation. (This is no longer true if $(q, n) > 1$.)

We may view $\sim_q$ as a refinement of $\sim$ in the following sense: thanks to the assumption that $(q, n) = 1$, $x \sim_q y$ always implies that $x \sim y$; the converse implication is often false. In general, if $\mathcal{C}(x)$ (resp., $\mathcal{C}_q(x)$) is the equivalence class of an element x of G w.r.t. $\sim$ (resp., $\sim_q$), then $\mathcal{C}(x) = \mathcal{C}_q(x)$ if and only if q is a generator of $(\mathbb{Z}/|\langle x\rangle|\mathbb{Z})^\times$.

We can now state our main result.

Theorem 1.2. *Let G be an abelian group of order $n \in \mathbb{N}^*$ and let p be a prime with $(p, n) = 1$. Let K be a finite extension of $\mathbb{Q}_p$ and let A_K, M_K and k be as defined above. Let $D \in A_K[G]$ and set $q := |k|$. Then $\chi(D) \in A_K$ for every character $\chi : G \to K(\xi_n)$(where ξ_n is a primitive nth root of unity) if and only if equivalent elements $x \sim_q y$ of G have equal coefficients in D (that is, D is constant on equivalence classes of G w.r.t. $\sim_q$).*

By combining Theorems 1.1 and 1.2 we obtain the following local-global principle for characters sums for a certain type of cyclic groups (see Section 4).

Theorem 1.3. *Let q_1 and q_2 be distinct primes and let $G = \langle a_1\rangle \times \langle a_2\rangle$ be a cyclic group of order $n = q_1q_2$ with $|\langle a_i\rangle| = q_i$ $(i = 1, 2)$. Let $D \in \mathbb{Z}[G]$. Then $\chi(D) \in \mathbb{Z}$ for every character $\chi : G \to \mathbb{C}^\times$ if and only if $\psi(D) \in \mathbb{Z}_p$ for every prime p and every character $\psi : G \to \mathbb{Q}_p(\xi_n)$ (where ξ_n is a primitive nth root of unity).*

2. Auxiliary results

To facilitate the proof of Theorem 1.2 we require several lemmas concerning irreducibility of polynomials over finite fields and over valuation rings of finite extensions of $\mathbb{Q}_p$. We start with the following fundamental result for which we provide a short proof.

Lemma 2.1. *Let $\mathbb{F}_q$ be a finite field with q elements (where q is a power of a prime p). Fix $n \in \mathbb{N}^*$ and write $n = p^r m$, where $(p, m) = 1$. Set $d := \mathrm{ord}_m(q)$. Let ξ_n be a root of the nth cyclotomic polynomial $\Phi_n(X)$ in a splitting field of $X^n - 1$ over $\mathbb{F}_q$. Then the following holds:*

(i) *In $\mathbb{F}_q[X]$, $\Phi_n(X)$ decomposes as*

$$\Phi_n(X) = (P_1(X))^{p^r}(P_2(X))^{p^r}\cdots(P_{\frac{\varphi(m)}{d}}(X))^{p^r}$$

where each $P_i(X)$ is monic, irreducible over $\mathbb{F}_q$ and of degree d, and $P_1(X), \ldots, P_{\frac{\varphi(m)}{d}}(X)$ are pairwise distinct.

(ii) *$\mathbb{F}_q(\xi_n)$ is the splitting field of any such $P_i(X)$ and $|\mathbb{F}_q(\xi_n) : \mathbb{F}_q| = d$.*

(iii) *For $i = 0, \ldots, d-1$, the map $\sigma_i : \mathbb{F}_q(\xi_n) \to \mathbb{F}_q(\xi_n)$ defined by $x \mapsto x^{q^i}$ is a field automorphism of $\mathbb{F}_q(\xi_n)$ fixing $\mathbb{F}_q$.*

(iv) *If $P_i(X) = \prod_{j=1}^{d}(X - \alpha_j)$ (where each α_j is primitive nth root in a splitting field of $\Phi_n(X)$ over $\mathbb{F}_q$), then for any symmetric polynomial $Q(X_1, \ldots, X_d)$ in variables $X_1, \ldots, X_d$, $Q(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q$. In particular, $\alpha_1 + \alpha_2 + \cdots + \alpha_d \in \mathbb{F}_q$.*

Proof. Suppose first that $r = 0$ (i.e., $(p, n) = 1$ and $m = n$). Then $\Phi_n(X)$ is not divisible by the square of a non-constant polynomial in $\mathbb{F}_q[X]$ (since $X^n - 1$ is separable over a field of characteristic co-prime to n). Hence, it suffices to show that every irreducible factor of $\Phi_n(X)$ over $\mathbb{F}_q[X]$ is monic and of degree d. Let $P(X)$ be an irreducible factor of $\Phi_n(X)$ over $\mathbb{F}_q$ and suppose it is of degree $s \in \mathbb{N}^*$. Let ξ be a root of $P(X)$ (which is, by definition, a primitive nth root of unity). Let $K = \mathbb{F}_q(\xi)$ (note that $K \cong \mathbb{F}_q[X]/(P(X))$). Then, $|K| = q^s$ and $\xi^{q^s-1} = 1$. Hence, $q^s - 1 \equiv 0 \pmod{n}$, so s is a multiple of d and $s \geqslant d$.

Since $\xi^n = 1$ and $q^d \equiv 1 \pmod{n}$ (by definition), we have $\xi^{q^d} = \xi$. Consider the polynomial $Q(X) = X^{q^d} - X$ and let K' be the splitting field of $Q(X)$ over $\mathbb{F}_q$. Since $\xi \in K'$, it follows that K is a subfield of K' and so $q^s \leqslant q^d$ and $d \geqslant s$. Hence, $d = s$, as required.

If $r \geqslant 1$, then in $\mathbb{F}_q[X]$, we have $X^n - 1 = X^{p^r m} - 1 = (X^m - 1)^{p^r}$ (since $\mathbb{F}_q$ is of characteristic p). Now $X^m - 1$ decomposes in $\mathbb{F}_q[X]$ as above. This proves (i).

Items (ii)–(iv) follows in a straightforward manner by Item (i). $\square$

We need the following well-known version of Hensel's Lemma.

Theorem 2.2. *Let K be a finite extension of $\mathbb{Q}_p$ and let A_k, M_k and k be as defined in Section 1. Let $F(X) \in A_k[X]$ be a monic polynomial of degree n. Let $f_1(X), f_2(X) \in k[X]$ be distinct monic irreducible polynomials of respective degrees r and $n - r$ ($0 \leqslant r \leqslant n$) such that $\overline{f}(X) = f_1(X)f_2(X)$ (where for a polynomial $P(X) \in A_k[X]$, $\overline{P}(X)$ is the polynomial obtained from $P(X)$ by reducing its coefficients modulo M_k). Then there exist unique monic irreducible polynomials $F_1(X), F_2(X) \in A_k[X]$ of respective degrees r and $n - r$ such that $F(X) = F_1(X)F_2(X)$ and $\overline{F_i}(X) = f_i(X)$ (for $i = 1, 2$).*

We deduce,

Lemma 2.3. *Let K be a finite extension of $\mathbb{Q}_p$ and let A_K, M_K and k be as defined in Section 1. Set $q := |k|$. Let $m \in \mathbb{N}^*$ with $(p, m) = 1$, and let $K' := K(\xi_m)$ (where ξ_m is a primitive mth root of unity). Then the minimal polynomial of ξ_m over A_K is $P_{\xi_m}(X) = \prod_{j \in \langle q \rangle_m}(X - \xi_m^j)$. In particular, $\sum_{j \in \langle q \rangle_m} \xi_m^j \in A_K$.*

Proof. For the field K', let $A_{K'}$, $M_{K'}$, k' be as defined in Section 1. Set $d := \mathrm{ord}_m(q)$. Consider the mth cyclotomic polynomial $\Phi_m(X)$ as a polynomial with coefficient in $A_{K'}$. In $K'[X]$, $\Phi_m(X) = \prod_{1 \leqslant i \leqslant m, (i,m)=1}(X - \xi_m^i)$.

Let $\overline{\Phi}_m(X) \in k[X] \subseteq k'[X]$ by obtained from $\Phi_m(X)$ by reducing its coefficient modulo $M_{K'}$ and let $\overline{\xi_m} \in k'$ be obtained from ξ_m by reducing it modulo $M_{K'}$. (Note that $\xi_m \in A_{K'}$, so this is well-defined.) By Lemma 2.1, in $k[X]$

$$\overline{\Phi}_m(X) = \overline{P}_1(X)\overline{P}_2(X) \cdots \overline{P}_{\frac{\varphi(m)}{d}}(X)$$

where each $\overline{P}_i(X) \in k[X]$ is monic, irreducible over k and of degree d, and $\overline{P}_1(X), \ldots, \overline{P}_{\frac{\varphi(m)}{d}}(X)$ are pairwise distinct.

By Hensel's Lemma 2.2, there exist unique polynomials $P_1(X), \ldots, P_{\frac{\varphi(m)}{d}}(X) \in A_K[X] \subseteq A_{K'}[X]$ such that

$$\Phi_m(X) = P_1(X)P_2(X)\cdots P_{\frac{\varphi(m)}{d}}(X)$$

where $\overline{P}_i(X) \equiv P_i(X) \pmod{M_{K'}}$, and each $P_i(X)$ is monic, irreducible over A_K and of degree d.

Since ξ_m is a root of $\Phi_m(X)$, there exists $1 \leqslant i \leqslant \frac{\varphi(m)}{d}$ with $P_i(\xi_m) = 0$ so that $\overline{P}_i(\overline{\xi_m}) = 0$. By Lemma 2.1(ii)–(iii), $\overline{P}_i(X) = \prod_{j\in\langle q\rangle_m}(X - \overline{\xi_m}^j)$. Hence, the uniqueness of $P_i(X)$ implies that $P_i(X) = \prod_{j\in\langle q\rangle_m}(X - \xi_m^j)$. The first assertion follows (with $P_{\xi_m}(X) = P_i(X)$) since $P_i(X)$ is irreducible over A_K and $P_i(\xi_m) = 0$.

For the second assertion set $\alpha := \sum_{j\in\langle q\rangle_m} \xi_m^j$. By Lemma 2.1(iv), $\overline{\alpha} \in k[X] = A_K/M_K'$ (where $\overline{\alpha}$ is the reduction of α modulo $M_{K'}$). Since K' is unramified over K (because p does not divide m) it follows that $\alpha \in A_K$ as claimed. □

Remark . Consider the settings of Lemma 2.3. Let $\mu_{(p)}(K) \subseteq K^\times$ be the group of roots of unity having order prime to p in K. It is well-known that the order of the cyclic group $\mu_{(p)}(K)$ is exactly $q-1$ [2, Chapter 2, Proposition 4.3.2]. This is a special case of Lemma 2.3 (with $m=1$ and $K'=K$). Indeed, if ξ_n is a primitive nth root of unity (with $(p,n)=1$) then $\xi_n \in A_K \Longleftrightarrow P_{\xi_n}(X) = \sum_{j\in\langle q\rangle_n}(X-\xi_n^j) = X-\xi_n$ $\Longleftrightarrow \mathrm{ord}_n(q) = 1$ (this is well-defined since $(p,n)=1$ so $(q,n)=1$) $\Longleftrightarrow n|(q-1)$. So $\xi_n \in A_K$ $\Longleftrightarrow \xi_n$ is a $(q-1)$th root of unity.

3. Proof of Theorem 1.2

In this section we prove Theorem 1.2. Let $K' := K(\xi_n)$ and let $A_{K'}, M_{K'}, k'$ be as defined in Section 1. Since K' is of characteristic zero, the left-regular representation of G is completely reducible. Let $G^* = \{\chi_1, \ldots, \chi_n\}$ be the set of characters of G (that is, the set of all distinct homomorphisms from G to the multiplicative group of K').

Let F be the $n \times n$ matrix with rows indexed by the χ_i's and columns indexed by the elements of G defined by $F_{(\chi_i,x)} := \chi_i(x)$ ($\chi_i \in G^*, x \in G$). By the orthogonality of the characters, $FF^* = nI_n$ (where F^* is the matrix obtained from the transpose of F by taking inverses cell-wise). We may now turn to the proof of Theorem 1.2.

Necessity. Let $D \in A_K[G]$ so that $\chi(D) \in A_K$ for every $\chi \in G^*$. Let $v \in (A_K)^n$ be the coefficients vector of D indexed by the elements of G in a way that is consistent with the indexing of the columns of F. For $x \in G$, we denote by v_x the xth coordinate of v (that is, the coefficient of x in D). By assumption, there exists a vector $z \in (A_K)^n$ such that

$$Fv = z \tag{1}$$

Fix $x \in G$ and set $m := |\langle x\rangle|$ and $d := \mathrm{ord}_m(q)$ (this is well-defined since $(q,n)=1$ so $(q,m)=1$). To complete the proof of the necessity part we have to show that x and x^ℓ have equal coefficients in D for every $\ell \in \langle q\rangle_m$.

By Eq. (1) and using F^*, we have $v_x = \dfrac{1}{n}\sum_{i=1}^n \chi_i(x)^{-1}z_i$ and $v_{x^\ell} = \dfrac{1}{n}\sum_{i=1}^n \chi_i(x^\ell)^{-1}z_i = \dfrac{1}{n}\sum_{i=1}^n \chi_i(x)^{-\ell}z_i$. Since x is of order m in G, each $\chi_i(x)$ is an mth root of unity. Since D has coefficients in A_K we may write:

$$v_x = \frac{1}{n}\sum_{i=0}^{m-1} \xi_m^i a_i \in A_K[\xi] \tag{2}$$

where $\xi_m \in K'$ is a primitive mth root of unity and $a_i \in A_K$ ($i = 0, \ldots, m-1$).

Consider the group Γ_m of mth roots of unity in K'. Since Γ_m is of order m and $(\ell, m) = 1$, the map $g \mapsto g^\ell$ (for $g \in \Gamma_m$) is an automorphism of Γ_m. Hence, using Eq. (2) we see that:

$$v_{x^\ell} = \frac{1}{n}\sum_{i=0}^{m-1}(\xi_m^\ell)^i a_i \in A_K[\xi_m] \tag{3}$$

Set

$$Q(X) := v_x - \frac{1}{n}\sum_{i=0}^{m-1} a_i X^i \in A_K[X] \tag{4}$$

By definition, $Q(\xi_m) = 0$.

Let $P_{\xi_m}(X)$ be the minimal polynomial of ξ_m over A_K as obtained in Lemma 2.3. Then $P_{\xi_m}(X)$ divides $Q(X)$ in $A_k[X]$. Hence, for $i \in \langle q\rangle_m$, ξ_m^i is also a root of $Q(X)$. Since $\ell \in \langle q\rangle_m$, it follows that $Q(\xi_m^\ell) = v_x - \frac{1}{n}\sum_{i=0}^{m-1}(\xi_m^\ell)^i a_i = 0$. Hence, by Eq. (3), $v_x = v_{x^j}$ as claimed. This completes the proof of the necessity part.

Sufficiency. Suppose that for every $x \in G$, D is constant on $\mathcal{C}_q(x)$. Fix $\chi \in G^*$ and $x \in G$. Set $m := |\langle x\rangle|$ and $d := \mathrm{ord}_m(q)$. It suffices to show that $\sum_{i\in\langle q\rangle_m}\chi(x^i) \in A_K$.

Since x is of order m, there exists $k \in \mathbb{N}^*$ with $k|m$ such that $\chi(x) = \xi_m^k$ (where $\xi_m \in K'$ is a primitive mth root of unity). Now,

$$\sum_{i\in\langle q\rangle_m}\chi(x^i) = \sum_{i\in\langle q\rangle_m}(\chi(x))^i = \sum_{i\in\langle q\rangle_m}(\xi_n^k)^i$$

Let $d' := \mathrm{ord}_{m/k}(q)$. Then $d = cd'$ for some $c \in \mathbb{N}^*$. Hence,

$$\sum_{i\in\langle q\rangle_m}(\xi_m^k)^i = \sum_{i=0}^{c-1}\sum_{j=d'i}^{d'i+d'-1}(\xi_m^k)^{q^j} = \sum_{i=0}^{c-1}\sum_{j=d'i}^{d'i+d'-1}(\xi_m^k)^{q^j \bmod (m/k)} \in A_K$$

The last containment follow from Lemma 2.3. This completes the proof.

4. Proof of Theorem 1.3

In this section we prove Theorem 1.3. We start with the following lemma (see, e.g., [3]) concerning sums of primitive roots of unity (also known as Ramanujan's sums).

Lemma 4.1. *Let K be either $\mathbb{Q}$ or $\mathbb{Q}_p$. Let G be an abelian group of order n and let $D \in 0/1[G]$ be the sum of elements of an equivalence class of G w.r.t. $\sim$. Then $\chi(D) \in \mathbb{Z}$ for every character $\chi : G \to K(\xi_n)$ (where ξ_n is a primitive nth root of unity).*

Using Lemma 4.1 and Theorem 1.2 we deduce the following:

Lemma 4.2. *Let q_1 and q_2 be distinct primes and let $G = \langle a_1\rangle \times \langle a_2\rangle$ be a cyclic group of order $n = q_1q_2$ with $|\langle a_i\rangle| = q_i$ ($i = 1, 2$). Let $D \in \mathbb{Z}[G]$. Then $\chi(D) \in \mathbb{Z}_p$ for every prime p and every character $\chi : G \to \mathbb{Q}_p(\xi_n)$ if and only if D is constant on equivalence classes w.r.t. $\sim$.*

Proof. If D is constant on equivalence classes then the claim follows by Lemma 4.1 and the assumption that the coefficients of D are in $\mathbb{Z}$.

For the converse, suppose that $\chi(D) \in \mathbb{Z}_p$ for every prime p and every character $\chi : G \to \mathbb{Q}_p(\xi_n)$. The proof is by induction on n.

If $n = 1$ the claim holds trivially. Suppose that the claim holds for G' and D' satisfying the assumptions of the theorem where G' is of order $< n$. Let $x \in G$ be a generator of (the cyclic group) G.

Claim 1. *D* is constant on $\mathcal{C}(x)$.

Subproof. Let $y \in G$ such that $y \sim x$. By definition of $\sim$, there exists $\ell \in \mathbb{N}^*$ with $(\ell, n) = 1$ and $y = x^\ell$. Write $\ell = \prod_{i=0}^{k} p_i^{k_i}$, where $k \in \mathbb{N}$, $p_0 := 1, p_1, \ldots, p_k$ are pairwise distinct prime divisors of ℓ, and $k_i \in \mathbb{N}^*$ (for $i = 0, \ldots, k$). For $i = 0, \ldots, k$, set $d_i := \mathrm{ord}_n(p_i)$ and choose $0 \leqslant \alpha_i \leqslant d_i - 1$ such that $\ell \equiv \prod_{i=0}^{k} p_i^{\alpha_i} \pmod n$. For $i = 0, \ldots, k$, set $\beta(i) := \prod_{j=0}^{i} p_j^{\alpha_j}$.

Since $x = x^\ell = x^{\ell \pmod n}$, to complete the proof of the claim we have to show that x and $x^{\ell \pmod n}$ have equal coefficients in D. To that goal we show that if $0 \leqslant i \leqslant k$, then x and $x^{\beta(i)}$ have equal coefficients in D.

We proceed by induction on i. If $i = 0$ (and then $\ell = 1$) this holds trivially. Suppose then that for every $1 \leqslant i < k$, x and $x^{\beta(i)}$ have equal coefficients in D. By assumption, $\chi(D) \in \mathbb{Z}_{p_{i+1}}$ for every character $\chi : G \to \mathbb{Q}_{p_{i+1}}(\xi_n)$. By Theorem 1.2, D is constant on equivalence classes w.r.t. $\sim_{p_{i+1}}$, and hence $x^{\beta(i)}$ and $x^{\beta(i) p_{i+1}^{\alpha_{i+1}}}$ have equal coefficients in D. Hence, x and $x^{\beta(i+1)}$ have equal coefficients in D. This proves Claim 1.

Now fix a prime p and a character $\chi : G \to \mathbb{Q}_p(\xi_n)$. Set $G_i := \langle a_i \rangle \leqslant G$ $(i = 1, 2)$. By Claim 1, $D = \gamma \mathcal{C}(x) + D_1 + D_2$, where the $\gamma \in \mathbb{Z}$ and $D_i \in \mathbb{Z}[G_i]$ $(i = 1, 2)$. (Note that G has exactly four equivalence classes of sizes $(q_1 - 1)(q_2 - 1)$, $q_1 - 1$, $q_2 - 1$ and 1.) By Lemma 4.1, $\chi(\mathcal{C}(x)) \in \mathbb{Z}$. Hence,

$$\chi(D) - \gamma \chi(\mathcal{C}(x)) = \chi(D_1) + \chi(D_2) \in \mathbb{Z} \tag{5}$$

For $i = 1, 2$, $\chi(D_i) \in \mathbb{Q}(\xi_{q_i})$ since the restriction of χ to G_i takes values in $\mathbb{Q}(\xi_{q_i}) \subset \mathbb{Q}_p(\xi_n)$. Now from the right-hand side of Eq. (5), the fact that $\mathbb{Q}(\xi_{q_1}) \cap \mathbb{Q}(\xi_{q_2}) = \mathbb{Q}$ and since $\chi(D_i)$ is an algebraic integer, it follows that $\chi(D_i) \in \mathbb{Z}$.

It is well-known that every character $\psi : G_i \to \mathbb{Q}_p(\xi_n)$ is the restriction to G_i of some character $\chi : G \to \mathbb{Q}_p(\xi_n)$ $(1 \leqslant i \leqslant 2)$. Since p and χ were arbitrary, we conclude that $\psi(D_i) \in \mathbb{Z}$ for every prime p and every character $\psi : G_i \to \mathbb{Q}_p(\xi_n)$. Since $q_i < n$, by induction, D_i is constant on equivalence classes w.r.t. to $\sim$. Hence, D is constant on equivalence classes w.r.t. $\sim$. $\square$

Proof of Theorem 1.3. The proof follows by Theorem 1.1 and Lemma 4.2.

Acknowledgement

The author would like to thank the anonymous referee for pointing out a gap in the proof of Lemma 2.3 and for many comments and suggestions that significantly improved the presentation of the paper.

References

[1] W. Bridges, R. Mena, Rational g-matrices with rational eigenvalues, Journal of Combinatorial Theory, Series A 32 (2) (1982) 264–280.
[2] A.M. Robert, A course in p-adic analysis, Springer, New York, NY, 2000.
[3] W. So, Integral circulant graphs, Discrete Mathematics 306 (1) (2006) 153–158.