FINITE-ORDER AUTOMORPHISMS OF A CERTAIN TORUS

BRIAN CONRAD

1. Introduction

A classical result of Higman [H], [S, Exer. 6.3], asserts that the roots of unity in the group ring $\mathbf{Z}[\Gamma]$ of a finite commutative group Γ are the elements $\pm\gamma$ for $\gamma \in \Gamma$. One application of this result is the determination of the group of finite-order automorphisms of a torus $T = \mathrm{Res}_{S'/S}(\mathbf{G}_m)$ for a finite étale Galois covering $f : S' \to S$ with S and S' connected schemes and abelian Galois group $\Gamma = \mathrm{Gal}(S'/S)$ (*e.g.*, an unramified extension of local fields). Indeed, the torus T has character group $\mathbf{Z}[\mathrm{Gal}(S'/S)]$ with $\mathrm{Gal}(S'/S)$ acting through left translation, and an automorphism of T is "the same" as an automorphism of its character group $\mathrm{X}(T)$ as a Galois module. Thus, to give an automorphism of T is to give a generator of $\mathbf{Z}[\mathrm{Gal}(S'/S)]$ as a left module over itself. This in turn is just a unit in the group ring. Once we have the list of roots of unity, this gives the list of finite-order automorphisms. It follows that the group of finite-order automorphisms of the torus T is the finite group that is generated (as a direct product) by inversion and the action of $\mathrm{Gal}(S'/S)$.

Now consider the problem (raised to the author by G. Prasad) of finding all finite-order automorphisms of the norm-1 subtorus T^1 in T when Γ is cyclic (*e.g.*, the Galois group of an unramified extension of local fields). This subtorus is functorially described as the kernel of the determinant map

$$\det : T = f_*\mathbf{G}_{m/S'} \to \mathbf{G}_{m/S};$$

for example, $T^1(S)$ is the group of units u on S' such that $\mathrm{N}_{S'/S}(u) = 1$ on S. The character group $\mathrm{X}(T^1)$ is the quotient of $\mathrm{X}(T)$ by the determinant character. Thus, if Γ is cyclic then $\mathrm{X}(T^1)$ is the Galois module

$$\mathbf{Z}[\Gamma]/(\sum_{\gamma\in\Gamma}\gamma) \simeq \mathbf{Z}[x]/(s_m),$$

where $\Gamma = \mathrm{Gal}(S'/S)$ has a chosen generator x and

$$s_m := x^{m-1} + \cdots + x + 1,$$

with $m = \deg(S'/S) = |\Gamma|$. Hence, in order to find all finite-order automorphisms of the norm-1 torus T^1 we are led to try to find all roots of unity in the order $\mathbf{Z}[x]/(s_m) \subseteq \prod_{d|m,d>1} \mathbf{Z}[\zeta_d]$. Of course, we expect to get the same answer as in the case of T, namely the product of the subgroup generated by inversion and the subgroup given by the action of $\mathrm{Gal}(S'/S)$. Note that for $m = 2$ the non-trivial element of $\mathrm{Gal}(S'/S)$ acts by inversion, but for $m > 2$ there are no non-trivial relations between inversion and the $\mathrm{Gal}(S'/S)$-action.

Unfortunately, the clever method of Higman for determining the roots of unity in $\mathbf{Z}[\Gamma]$ uses trace operators whose definition makes essential use of the group-ring structure. This technique does not seem to generalize to apply to the ring $\mathbf{Z}[x]/(s_m)$ that is not a group ring. Thus, in order to solve the above problem, we need to find a different method. The geometric method of filtering a norm-1 torus by norm-1 tori relative to steps of a Galois tower (so as to try to reduce immediately to the easy prime-degree case, for example) seems to quickly run into difficulties, especially if we want to keep track of automorphisms of order 2. Thus, we are forced to adopt an algebraic approach.

Date: September 14, 2003.

1991 *Mathematics Subject Classification.* Primary 20G35.

Key words and phrases. group ring, torus automorphism.

This work was supported by the NSF and the Alfred P. Sloan Foundation. I would like to thank G. Prasad for raising the question considered here.

In brief, we view rings such as $\mathbf{Z}[x]/(s_m)$ and $\mathbf{Z}[x]/(x^m-1) = \mathbf{Z}[\Gamma]$ as obtained by gluing certain closed subschemes of the affine line $\mathbf{A}^1_{\mathbf{Z}}$ along various artinian overlaps. By means of suitable induction arguments which follow the geometry of this gluing, we are able to solve the problem by inducting on the prime factorization of m. Although most of our motivation and reasoning is inspired by thinking in terms of schemes, the proofs use only the language of ring theory and (for the benefit of readers who do not use the framework of schemes) in statements of lemmas and theorems we provide ring-theoretic translations of scheme-theoretic statements.

It seems that a new idea is needed to handle the evident analogue of the motivating torus automorphism problem even for the most basic non-cyclic case $\Gamma = \mathbf{Z}/p \times \mathbf{Z}/p$. Here is the main result of this note, answering Prasad's question affirmatively in the cyclic case.

Theorem 1.1. *Let $n, m \geq 1$ be relatively prime positive integers with $m > 1$. Let $\mathbf{Z}'$ be the localization of $\mathbf{Z}$ at a multiplicative set of nonzero integers whose elements are relatively prime to m. Let $\mu_{\mathrm{tor}}(R)$ denote the group of roots of unity in a commutative ring R. For $m > 2$, the natural multiplication map*

$$\mu_{\mathrm{tor}}(\mathbf{Z}[\zeta_n]) \times \mu_m \rightarrow \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^{m-1} + \cdots + x + 1)) \tag{1.1}$$

is an isomorphism, where μ_m is a cyclic group of order m generated by x. When $m = 2$, this map is surjective with order-2 kernel that has $(-1,-1) = (-1,x)$ as its unique non-trivial element.

The use of the notation $\mathbf{Z}'$ suppresses the dependence on the choice of multiplicative set (that in turn is constrained by the choice of m), but for inductive divisibility arguments this ambiguity is not confusing and for expository purposes this imprecise notation makes things easier to read. Though the version of Theorem 1.1 using only $\mathbf{Z}' = \mathbf{Z}$ (and $n = 1$) is all that is required for Prasad's question, and it can be proved without localizing (but still requiring the generality of arbitrary n), allowing for localization in the inductive hypothesis eliminates some tedious considerations that are otherwise needed to pass from the case of prime-power m to the general case. This is the main reason for allowing denominators (avoiding the prime factors of m) in (1.1).

It is obvious that (1.1) is injective when $m > 2$, and the case $m = 2$ is trivial (but is convenient to include in the statement of the theorem for purposes of induction). It is also worth mentioning at the outset that even though the case $n = 1$ is the only one that is relevant for applications to torus automorphisms, the inductive method of proof requires us to treat the case of general $n \geq 1$. Actually, a preliminary result that we will need in the proof of Theorem 1.1 is a generalization of Higman's result with $\mathbf{Z}'[\zeta_n]$-coefficients: the group of roots of unity in $\mathbf{Z}'[\zeta_n][x]/(x^m - 1)$ for relatively prime positive integers n and m is the direct product of $\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) = \mu_{\mathrm{tor}}(\mathbf{Z}[\zeta_n])$ and the order-m group generated by x (see Theorem 3.1).

An extension of our localization arguments reduces the case of general abelian Γ to the case of Γ with prime-power order. Since we cannot prove anything even when Γ is a product of two cyclic groups of prime order p, nor do we see how to reduce the p-primary case to the p-torsion case, we have decided to omit discussion of the reduction of the general abelian case to the primary case. The interested reader should have no difficulty generalizing our localization arguments to establish this reduction step.

Notation. For a positive integer n and a commutative ring R, we write $R[\zeta_n]$ to denote $R \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_n] = R[X]/(\Phi_n)$, where Φ_n denotes the nth cyclotomic polynomial. Thus, for $R = \mathbf{Z}[\zeta_n]$ with n relatively prime to m we have $R[\zeta_m] = \mathbf{Z}[\zeta_{nm}]$, but for most R the ring $R[\zeta_m]$ is not a domain.

For any commutative ring R, we write $R^\times$ to denote the group of units in R and $\mu_{\mathrm{tor}}(R)$ to denote the torsion subgroup in $R^\times$ (*i.e.*, the roots of unity in R).

If $g \in G$ is an element in a group, we write $\langle g \rangle$ to denote the subgroup generated by g.

If S is a finite set, we write $\#S$ to denote the size of S.

2. Gluing subschemes of the affine line

The reader who prefers to avoid schemes should read (2.1) and then skip ahead to Lemma 2.2.

If we view $\mathrm{Spec}(\mathbf{Z}[x]/(x^n-1))$ and $\mathrm{Spec}\,\mathbf{Z}[\zeta_d] = \mathrm{Spec}(\mathbf{Z}[x]/\Phi_d)$ for $d|n$ as closed subschemes of $\mathbf{A}^1_{\mathbf{Z}}$, then $\mathrm{Spec}(\mathbf{Z}[x]/(x^n-1))$ is physically the union of the $\mathrm{Spec}(\mathbf{Z}[\zeta_d])$'s. More precisely, the natural map

$$\coprod_{d|n} \mathrm{Spec}(\mathbf{Z}[\zeta_d]) \to \mathbf{A}^1_{\mathbf{Z}}$$

factors through $\mathrm{Spec}(\mathbf{Z}[x]/(x^n-1))$, so if Z denotes the scheme-theoretic image of this map then we get a closed immersion $i : Z \hookrightarrow \mathrm{Spec}(\mathbf{Z}[x]/(x^n-1))$ between finite flat reduced $\mathbf{Z}$-schemes, and i is an isomorphism over $\mathbf{Q}$ (or even over $\mathbf{Z}[1/n]$), so it must be an isomorphism. However, it is important for our purposes to know the mechanism by which $\mathrm{Spec}(\mathbf{Z}[x]/(x^n-1))$ is obtained by gluing the $\mathrm{Spec}(\mathbf{Z}[\zeta_d])$'s along artinian closed overlaps.

Due to lack of an adequate reference, let us recall some standard terminology that serves primarily as geometric motivation for our method of proof of Theorem 1.1. We formulate the following definition in a general setting because the relevant construction is easier to carry out without having to worry at the same time whether we are remaining within the category of schemes.

Definition 2.1. Let Y and Y' be two ringed spaces, and let $i : Z \hookrightarrow Y$ and $i' : Z \hookrightarrow Y'$ be two closed immersions. We define a *gluing of Y and Y' along Z* to be a commutative diagram of ringed spaces

$$\begin{tikzcd} Z \arrow[r, "i"] \arrow[d, "i'"'] & Y \arrow[d, "j"] \\ Y' \arrow[r, "j'"'] & Y \coprod_Z Y' \end{tikzcd}$$

such that for any pair of maps $f : Y \to W$, $f' : Y' \to W$ to another ringed space with $f \circ i = f' \circ i'$, there exists a unique map $F : Y \coprod_Z Y' \to W$ such that $F \circ j = f$, $F \circ j' = f'$.

The existence and uniqueness of a gluing is simple: we define $Y \coprod_Z Y'$ to be the gluing on underlying topological spaces along i and i' (using the quotient topology), so topologically j and j' are the evident maps. Letting $k = j \circ i = j' \circ i'$ on the level of topological spaces, we define the sheaf of rings

$$\mathscr{O}_{Y \coprod_Z Y'} = j_* \mathscr{O}_Y \times_{k_* \mathscr{O}_Z} j'_* \mathscr{O}_{Y'},$$

where for a pair of ring maps $\alpha : A \to C$ and $\beta : B \to C$ we define the *fiber-product ring*

$$A \times_C B \overset{\mathrm{def}}{=} \{(a,b) \in A \times B \,|\, \alpha(a) = \beta(b)\} \subseteq A \times B. \tag{2.1}$$

It is easy to check (with the evident maps on sheaves of rings) that this construction satisfies the universal property to be a gluing, so in particular the maps j and j' in the universal property are closed immersions and have intersection (in the ringed space sense) equal to Z, and moreover the formation of such gluing is of local nature on Y and Y' (relative to Z). More specifically, if $U \subseteq Y$ and $U' \subseteq Y'$ are opens that meet Z in a common open $V \subseteq Z$, then there is a natural map

$$U \coprod_V U' \to Y \coprod_Z Y'$$

that is an open immersion.

Due to the local behavior, it is clear from the construction that if the setup is given in the category of locally ringed spaces then the gluing is a locally ringed space and its universal data also makes it universal in the category of locally ringed spaces. With these observations made, we claim that the category of schemes is stable under such gluing. By working locally, we reduce to the affine case, and the problem comes down to proving that for a pair of *surjective* ring maps $\alpha : A \to C$ and $\beta : B \to C$, the natural map of locally ringed spaces

$$\mathrm{Spec}(A) \coprod_{\mathrm{Spec}(C)} \mathrm{Spec}(B) \to \mathrm{Spec}(A \times_C B) \tag{2.2}$$

is an isomorphism. Topologically the situation is clear (since α and β are surjective), and for the sheaf aspect we can therefore work locally. By judicious use of basic open affines, we thereby reduce to the claim that

(2.2) induces an isomorphism on global sections, and this is clear from how the structure sheaf on the left side is defined.

We note in passing that if all of the gluing data is given over a base scheme S, so the gluing $Y\coprod_Z Y'$ is universal in the category of S-schemes, we can then inquire about the base-change compatibility of this construction. Compatibility with flat base change is clear, and this is the only aspect we shall need (compatibility with respect to base change also holds if Z is S-flat).

The real purpose of going through this formalism is to give geometric meaning to the following easy but crucial algebraic result that mildly generalizes the Chinese remainder theorem.

Lemma 2.2. *Let C be a domain with fraction field K, and let $f,g\in C[x]$ be two monic polynomials which are relatively prime in $K[x]$. The natural C-algebra map*

$$C[x]/(fg)\to C[x]/(f)\times_{C[x]/(f,g)} C[x]/(g)$$

is an isomorphism. That is, the closed subscheme $\operatorname{Spec}(C[x]/(fg))\hookrightarrow \mathbf{A}^1_C$ *is the gluing of* $\operatorname{Spec}(C[x]/(f))$ *and* $\operatorname{Spec}(C[x]/(g))$ *along their overlap* $\operatorname{Spec}(C[x]/(f,g))$ *inside of* $\mathbf{A}^1_C$*.*

Proof. Since the source is finite free as a C-module, for injectivity we may check after flat extension of scalars to K, where the map is clearly an isomorphism by the usual Chinese remainder theorem. As for surjectivity, if $a\in C[x]$ and $b\in C[x]$ represent respective elements $\overline{a}\in C[x]/(f)$ and $\overline{b}\in C[x]/(g)$ with the same image in $C[x]/(f,g)$, then $a+f\psi=b+g\phi$ for some $\psi,\phi\in C[x]$. This gives an element in $C[x]/(f,g)$ mapping to the chosen element $(\overline{a},\overline{b})$ in the fiber product ring. ■

We wish to give two examples of Lemma 2.2 that will be used later. As a first example, we fix a prime p and a positive integer e. Also choose a domain C with characteristic not equal to p. We will be interested in the case $C=\mathbf{Z}'[\zeta_n]$ with n not divisible by p (and $\mathbf{Z}'$ a localization of $\mathbf{Z}$). We want to describe $\operatorname{Spec} C[x]/(x^{p^e}-1)$ as a gluing of $\operatorname{Spec} C[x]/(x^{p^{e-1}}-1)$ and $\operatorname{Spec} C[\zeta_{p^e}]$ along suitable closed subschemes. If we write $\overline{C}$ to denote C/p, then there are canonical surjections

$$C[x]/(x^{p^{e-1}}-1)\twoheadrightarrow \overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}})\twoheadleftarrow C[\zeta_{p^e}]$$

defined by

$$x\mapsto 1+\varepsilon,\ \ \zeta_{p^e}\mapsto 1+\varepsilon.$$

Lemma 2.3. *The scheme-theoretic intersection of* $\operatorname{Spec}(C[x]/(x^{p^{e-1}}-1))$ *and* $\operatorname{Spec}(C[\zeta_{p^e}])$ *inside of* $\mathbf{A}^1_C$ *is exactly* $\operatorname{Spec}(\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}})))$*, and the natural map*

$$\operatorname{Spec}(C[x]/(x^{p^{e-1}}-1))\coprod_{\operatorname{Spec}(\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}}))}\operatorname{Spec}(C[\zeta_{p^e}])\to\operatorname{Spec}(C[x]/(x^{p^e}-1))$$

is an equality of closed subschemes of $\mathbf{A}^1_C$.

In other words, the map

$$C[x]/(x^{p^e}-1)\to C[x]/(x^{p^{e-1}}-1)\times_{\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}})} C[\zeta_{p^e}] \tag{2.3}$$

defined by $x\mapsto(x,\zeta_{p^e})$ is an isomorphism of C-algebras.

Proof. Since the fraction field K of C has charateristic not equal to p, clearly $x^{p^{e-1}}-1$ and Φ_{p^e} are relatively prime in $K[x]$. Thus, the hypotheses in Lemma 2.2 are satisfied, so we just have to check that the common quotient $\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}})$ of $C[x]/(x^{p^{e-1}}-1)$ and $C[\zeta_{p^e}]$ is exactly $C[x]/(x^{p^{e-1}}-1,\Phi_{p^e})$. It suffices to check the case $C=\mathbf{Z}$; we have

$$\mathbf{Z}[x]/(x^{p^{e-1}}-1,\Phi_{p^e})\simeq\mathbf{Z}[\zeta_{p^e}]/(\zeta_p-1), \tag{2.4}$$

and ramification theory for cyclotomic fields [W, Ch 1] identifies this latter ring with $\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}})$, where $\varepsilon=1+\zeta_{p^e}$. This completes the proof, and we also note that the common quotient (2.4) is the unique length-p^{e-1} artinian quotient of each of our rings $\mathbf{Z}[x]/(x^{p^{e-1}}-1)$ and $\mathbf{Z}[\zeta_{p^e}]$. ■

The other example of Lemma 2.2 concerns rings of the form

$$C_{p^e} = C[x]/(s_{p^e})$$

where $s_m = x^{m-1} + \cdots + x + 1$, with $e \geq 0$ (so $s_1 = 1$ and $C_1 = 0$). We again take C to be a domain with characteristic not equal to p and we define $\overline{C} = C/p$. For $e \geq 1$, we have natural surjections

$$C_{p^{e-1}} \twoheadrightarrow \overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}-1}) \twoheadleftarrow C[\varepsilon]$$

defined by

$$x \mapsto 1+\varepsilon, \quad \zeta_{p^e} \mapsto 1+\varepsilon.$$

The first map is well-defined because $s_{p^{e-1}} = (x-1)^{p^{e-1}-1}$ in $\mathbf{F}_p[x]$. In the special case $C = \mathbf{Z}$, these maps determine the unique length-$(p^{e-1}-1)$ artinian quotients of the rings $\mathbf{Z}[x]/(s_{p^{e-1}})$ and $\mathbf{Z}[\zeta_{p^e}]$.

Lemma 2.4. *For $e \geq 1$ and C a domain with characteristic not equal to p, the scheme-theoretic intersection of* $\mathrm{Spec}(C[x]/(s_{p^{e-1}}))$ *and* $\mathrm{Spec}(C[\zeta_{p^e}])$ *inside of $\mathbf{A}^1_C$ is exactly* $\mathrm{Spec}(\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}-1}))$*, and the natural map*

$$\mathrm{Spec}(C[x]/(s_{p^{e-1}})) \coprod_{\mathrm{Spec}(\overline{C}[\varepsilon]/\varepsilon^{p^{e-1}-1})} \mathrm{Spec}(C[\zeta_{p^e}]) \to \mathrm{Spec}(C[x]/(s_{p^e}))$$

is an equality of closed subschemes of $\mathbf{A}^1_C$. In other words,

$$C_{p^e} \to C_{p^{e-1}} \times_{\overline{C}[\varepsilon]/(\varepsilon^{p^{e-1}-1})} C[\zeta_{p^e}] \tag{2.5}$$

is an isomorphism of C-algebras.

The proof goes exactly like the proof of Lemma 2.3.

3. Roots of unity on a multiplicative group

As was noted in the Introduction, to prove Theorem 1.1 we will first need to determine the roots of unity in $\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ for relatively prime positive integers n and m (with $\mathbf{Z}'$ denoting a localization of $\mathbf{Z}$ with denominators avoiding prime factors of m). In fact, the treatment of this problem also serves as an easier context for carrying out the strategy of proof of Theorem 1.1. The essential simplifying aspect of this particular example is that inducting on the prime factorization of m is made feasible by means of the natural isomorphism of C-algebras

$$C[x]/(x^{m_1m_2}-1) \simeq C[x]/(x^{m_1}-1) \otimes_C C[x]/(x^{m_2}-1) \tag{3.1}$$

for relatively prime positive integers m_1 and m_2, defined via $x \mapsto x \otimes x$. Geometrically, this is just the canonical isomorphism of C-group schemes

$$\mu_{m_1} \times \mu_{m_2} \simeq \mu_{m_1m_2}$$

defined via multiplication.

Theorem 3.1. *For relatively prime positive integers n and m, the natural multiplication-map of groups*

$$\mu_{\mathrm{tor}}(\mathbf{Z}[\zeta_n]) \times \mu_m = \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_m \to \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^m-1)) \tag{3.2}$$

is an isomorphism, where $\mu_m := \langle x \rangle$ is cyclic of order m.

Proof. The case $m = 1$ is clear for all n, and the injectivity of (3.2) is clear in general. Thus, it is enough to prove that the right side of (3.2) has size at most that of the left side. Such counting will allow us to avoid having to make some isomorphisms explicit later on.

We will now treat the case when $m = p^e$ is a prime power (with $e \geq 1$), via Lemma 2.3 and induction on e. With $m = p^e$, we start the induction at the settled case $e = 0$. When $e \geq 1$ we have p not dividing n, and so we have a natural isomorphism

$$\mathbf{Z}'[\zeta_n] \otimes_{\mathbf{Z}'} \mathbf{Z}'[\zeta_{p^e}] \simeq \mathbf{Z}'[\zeta_{np^e}].$$

By Lemma 2.3 with $C = \mathbf{Z}'[\zeta_n]$ we therefore have a $\mathbf{Z}'[\zeta_n]$-algebra isomorphism

$$\mathbf{Z}'[\zeta_n][x]/(x^{p^e}-1) \simeq \mathbf{Z}'[\zeta_n][x]/(x^{p^{e-1}}-1) \times_{\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}})} \mathbf{Z}'[\zeta_{np^e}]$$

that carries x to (x, ζ_{p^e}). The projection-maps to $\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}})$ in the fiber-product ring are determined by $x \mapsto 1+\varepsilon$ and $\zeta_{p^e} \mapsto 1+\varepsilon$. Thus, we have a natural isomorphism

$$\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^{p^e}-1)) \simeq \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^{p^{e-1}}-1)) \times_{(\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}}))^\times} \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{np^e}]).$$

From the theory of cyclotomic fields, since $e \geq 1$ (so p does not divide n) we have

$$\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{np^e}]) = \begin{cases} \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_{p^e}, & \text{if } p \neq 2 \\ \mu_n \times \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{p^e}]), & \text{if } p = 2. \end{cases} \tag{3.3}$$

Combining this with the inductive hypothesis, we get

$$\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^{p^e}-1)) = \begin{cases} (\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_{p^{e-1}}) \times_{(\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}}))^\times} (\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_{p^e}), \text{if } p \neq 2 \\ (\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_{2^{e-1}}) \times_{(\mathbf{F}_2[\zeta_n][\varepsilon]/(\varepsilon^{2^{e-1}}))^\times} (\mu_n \times \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{2^e}])), \text{if } p = 2 \end{cases} \tag{3.4}$$

with the projection

$$\mu_{p^{e-1}} \to (\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}}))^\times \tag{3.5}$$

sending a generator x modulo $(x^{p^{e-1}}-1)$ to the element

$$1+\varepsilon \in (\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}}))^\times$$

that has multiplicative order exactly p^{e-1}. Thus, (3.5) is injective. Note also that in (3.4) we can replace $\mathbf{Z}'$ with $\mathbf{Z}$ on the right side without affecting the equalities. Since reduction mod p is also faithful on square roots and nth roots of unity when $p \neq 2$, it follows for odd p that the right side of (3.2) has size at most $p^e \cdot \#\mu_{\mathrm{tor}}(\mathbf{Z}[\zeta_n])$; this is the size of the left side of (3.2). Hence, (3.2) is an isomorphism when $m = p^e$ and $p \neq 2$, completing the induction on e in case m is an odd prime power.

For the case $p = 2$ (so n is odd), the second case of (3.4) yields

$$\begin{aligned} \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^{2^e}-1)) &= (\mu_n \times \mu_{\mathrm{tor}}(\mathbf{Z}') \times \mu_{2^{e-1}}) \times_{(\mathbf{F}_2[\zeta_n][\varepsilon]/(\varepsilon^{2^{e-1}}))^\times} (\mu_n \times \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{2^e}])) \\ &= \mu_n \times ((\langle -1 \rangle \times \mu_{2^{e-1}}) \times_{(\mathbf{F}_2[\varepsilon]/(\varepsilon^{2^{e-1}}))^\times} \mu_{2^e}), \end{aligned}$$

with $\mu_{2^{e-1}}$ generated by x modulo $x^{2^{e-1}}-1$. Since

$$\mu_{2^{e-1}} \to (\mathbf{F}_2[\varepsilon]/(\varepsilon^{2^{e-1}}))^\times$$

is defined by sending the generator x to $1+\varepsilon$, whereas the projection

$$\langle -1 \rangle \to (\mathbf{F}_2[\varepsilon]/(\varepsilon^{2^{e-1}}))^\times$$

is the trivial map, it follows that for $m = 2^e$ the right side of (3.2) has size at most

$$2^e \cdot 2n = m \cdot \#\mu_{\mathrm{tor}}(\mathbf{Z}[\zeta_n]),$$

that is the size of the left side of (3.2). Thus, (3.2) is an isomorphism whenever m is a power of 2. This settles the case when m a prime power.

Now we induct on the number of prime factors of m. More specifically, we may assume $m = m_1 m_2$ with relatively prime positive integers $m_j > 1$ such that (3.2) is known to be an isomorphism (for arbitrary n relatively prime to m_j), and we have to show that (3.2) is an isomorphism for $m = m_1 m_2$. It suffices to check surjectivity. By relabelling, we may assume m_1 is odd. Choose $z \in \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(x^m-1))$. The factor-fields of the

$$\mathbf{Q} \otimes_{\mathbf{Z}'} (\mathbf{Z}'[\zeta_n][x]/(x^m-1))$$

have the form $\mathbf{Q}(\zeta_{nd})$ for $d|m$ since $\gcd(n,m) = 1$, so $z^{2nm} = 1$ (as this holds for roots of unity in each factor field). Since m_1 is relatively prime to $2nm_2$, we can write $z = z_1 z_2$ where $z_1^{m_1} = 1$ and z_2 has order prime to m_1. It therefore suffices to separately treat the cases when z is an m_1th root of unity and when z has order prime to m_1.

Let us first consider the case when z has order prime to m_1. Inverting m_2 and defining $\mathbf{Z}'' = \mathbf{Z}'[1/m_2]$, (3.1) allows us to view z as a root of unity in the ring

$$\mathbf{Z}''[\zeta_n][x]/(x^{m_1}-1) \otimes_{\mathbf{Z}''[\zeta_n]} \mathbf{Z}''[\zeta_n][x]/(x^{m_2}-1).$$

Since $x^{m_2}-1$ is a monic polynomial over $\mathbf{Z}''$ with unit discriminant in $\mathbf{Z}''$, and $\gcd(m_2,n)=1$, we get

$$\mathbf{Z}''[\zeta_n][x]/(x^{m_2}-1)\simeq\prod_{d|m_2}\mathbf{Z}''[\zeta_{nd}],$$

so the natural map

$$\mathbf{Z}''[\zeta_n][x]/(x^m-1)\to\prod_{d|m_2}\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1) \tag{3.6}$$

defined by $x\mapsto(\zeta_d x)_{d|m_2}$ is an isomorphism. Thus, by the inductive hypothesis (for m_1 and the localization $\mathbf{Z}''$ away from m_1), if we write $z=(z_d)_{d|m_2}$ for the decomposition of z under (3.6), then each root of unity $z_d\in\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1)$ lies in the subgroup $\mu_{\rm tor}(\mathbf{Z}[\zeta_{nd}])\times\mu_{m_1}$ and has order prime to m_1. Thus, $z_d\in\mu_{\rm tor}(\mathbf{Z}[\zeta_{nd}])$ for all $d|m_2$.

For $a\in(\mathbf{Z}/m)^\times$ with $a\equiv 1 \bmod m_2$, the automorphism $\sigma_a: x\mapsto x^a$ of $\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ goes over (upon inverting m_2) to the componentwise automorphism that acts on $\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1)$ by fixing ζ_{nd} and sending x to x^a. These componentwise automorphisms leave z_d invariant, so $\sigma_a(z)=z$ in $\mathbf{Z}''[\zeta_n][x]/(x^m-1)$, and hence $\sigma_a(z)=z$ in $\mathbf{Z}'[\zeta_n][x]/(x^m-1)$. The subring of $\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ invariant under all such σ_a's is exactly $\mathbf{Z}'[\zeta_n][y_1]/(y_1^{m_2}-1)$ where $y_1=x^{m_1}$. Thus, by the inductive hypothesis for m_2 and the localization $\mathbf{Z}'$ we get

$$z\in\mu_{\rm tor}(\mathbf{Z}'[\zeta_m][y_1]/(y_1^{m_2}-1))\simeq\mu_{\rm tor}(\mathbf{Z}'[\zeta_n])\times\mu_{m_2},$$

where μ_{m_2} is generated by $y_1=x^{m_1}$. This settles the surjectivity problem for z of order prime to m_1.

Now we consider the remaining case when $z^{m_1}=1$. By oddness of m_1, each component

$$z_d\in\mu_{\rm tor}(\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1))\simeq\mu_{\rm tor}(\mathbf{Z}[\zeta_{nd}])\times\mu_{m_1}$$

lies in the subgroup μ_{m_1} generated by x. That is, $z_d=x^{e_d}$ for some unique $e_d\in\mathbf{Z}/m_1$. Under (3.6) we have $x\mapsto(\zeta_d x)_{d|m_2}$, so $x^{m_2}\mapsto(x^{m_2})_{d|m_2}$. Consider the automorphism of $\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ defined by $\sigma_a: x\mapsto x^a$ for $a\in(\mathbf{Z}/m)^\times$ with $a\equiv 1 \bmod m_1$. This induces the componentwise action on each $\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1)$ leaving x and ζ_n invariant but sending ζ_d to ζ_d^a. The element $z_d=x^{e_d}$ is invariant under this action, so $z\in\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ is invariant under all such σ_a's. Thus, z lies in the subring $\mathbf{Z}'[\zeta_n][y_2]/(y_2^{m_1}-1)$ for $y_2=x^{m_2}$. Since y_2 has image $(x^{m_2})_{d|m_2}$, by considering the unique representative for z by a polynomial in y_2 of degree at most m_1-1 we see that the components $z_d=x^{e_d}\in\mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1)$ must have $e_d\in\mathbf{Z}/m_1$ independent of d. If e denotes this common value and $m_2'\in(\mathbf{Z}/m_1)^\times$ is the multiplicative inverse of m_2, then $x^{m_2m_2'e}\in\mathbf{Z}'[\zeta_n][x]/(x^m-1)$ has dth component z_d for all d, so $z=x^{m_2m_2'e}$. Thus, z lies in the subgroup generated by x. ■

4. Proof of Theorem 1.1

The proof of Theorem 1.1 will be modelled on that of Theorem 3.1, using Lemma 2.4 to replace the role of Lemma 2.3. Our proof will actually use Theorem 3.1. The case $m=1$ is trivial (for all n), and the behavior for $m=2$ is also clear. We wish to once again first settle the prime power case $m=p^e$ by induction on e over variable n prime to p (requiring special care for $p=2$), and then we will use localization to deduce the general case.

We begin by treating the case when $m=p^e$ is a prime power with $e\geq 1$. The case $m=2$ is trivial, so we may assume $m>2$. In particular, (1.1) is injective for our m, so we can once again use counting arguments. Taking $C=\mathbf{Z}'[\zeta_n]$ with n not divisible by p (and $\mathbf{Z}'$ a localization away from p), Lemma 2.4 yields

$$\mu_{\rm tor}(\mathbf{Z}'[\zeta_n][x]/(s_{p^e}))\simeq\mu_{\rm tor}(\mathbf{Z}'[\zeta_n][x]/(s_{p^{e-1}}))\times_{(\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}-1}))^\times}\mu_{\rm tor}(\mathbf{Z}'[\zeta_{np^e}]), \tag{4.1}$$

determined by $x\mapsto(x,\zeta_{p^e})$. We first treat the case $p\neq 2$. When $p\neq 2$, then induction on e and (3.3) yield

$$\begin{aligned}\mu_{\rm tor}(\mathbf{Z}'[\zeta_n][x]/(s_{p^e})) &= (\mu_{\rm tor}(\mathbf{Z}'[\zeta_n])\times\mu_{p^{e-1}})\times_{(\mathbf{F}_p[\zeta_n][\varepsilon]/(\varepsilon^{p^{e-1}-1}))^\times}(\mu_{\rm tor}(\mathbf{Z}'[\zeta_n])\times\mu_{p^e})\\ &= \mu_{\rm tor}(\mathbf{Z}'[\zeta_n])\times(\mu_{p^{e-1}}\times_{(\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}-1}))^\times}\mu_{p^e}),\end{aligned}$$

with the generators $x \bmod s_{p^{e-1}}$ of $\mu_{p^{e-1}}$ and ζ_{p^e} of μ_{p^e} both mapping to $1+\varepsilon$ under the fiber-product projections. The map

$$\mu_{p^{e-1}} \to (\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}-1}))^\times$$

determined by $x \mapsto 1+\varepsilon$ is once again injective. Indeed, the case $e=1$ is clear, and for $e \geq 2$ we use that $p^{e-2} < p^{e-1}-1$ for $p \neq 2$ (this is false for $p=2$ with $e=2$). Thus, the group

$$\mu_{p^{e-1}} \times_{(\mathbf{F}_p[\varepsilon]/(\varepsilon^{p^{e-1}-1}))^\times} \mu_{p^e}$$

has size at most p^e, so the right side of (1.1) has size at most $p^e \cdot \#\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n])$; this is the size of the left side of (1.1). It follows that (1.1) is an isomorphism for $m = p^e$ with p an odd prime.

For the case $p=2$ (so n is odd), we have $e \geq 2$ since $p^e = m > 2$. By (4.1),

$$\begin{aligned} \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n][x]/(s_4)) &= \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times_{(\mathbf{F}_2[\zeta_n])^\times} \mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_{4n}]) \\ &= \mu_n \times (\langle -1 \rangle \times \mu_4), \end{aligned}$$

and this has size $8n$, and $8n$ is also the size of the left side of (1.1) when $m=4$. Finally, for $p=2$ and $e>2$, the natural map

$$\mu_{2^{e-1}} \to (\mathbf{F}_2[\varepsilon]/(\varepsilon^{2^{e-1}-1}))^\times$$

defined by $x \mapsto 1+\varepsilon$ is injective since $e-1 \geq 2$, whence we compute that $\mathbf{Z}'[\zeta_n][x]/(s_{2^e})$ has group of roots of unity equal to

$$(\mu_{\mathrm{tor}}(\mathbf{Z}'[\zeta_n]) \times \mu_{2^{e-1}}) \times_{(\mathbf{F}_2[\zeta_n][\varepsilon]/(\varepsilon^{2^{e-1}-1}))^\times} (\mu_n \times \mu_{2^e}) = \mu_n \times ((\langle -1 \rangle \times \mu_{2^{e-1}}) \times_{(\mathbf{F}_2[\varepsilon]/(\varepsilon^{2^{e-1}-1}))^\times} \mu_{2^e}),$$

and by noting that the first projection in the fiber product has kernel $\langle -1 \rangle$ of order 2, we conclude that the group of roots of unity in $\mathbf{Z}'[\zeta_n][x]/(s_{2^e})$ has size at most $n \cdot 2 \cdot 2^e$. But this is exactly the size of the left side of (1.1), so (1.1) must be an isomorphism when $m = 2^e$. This settles the case in which m is a prime power.

To handle the case when m has more than one prime factor, the problem is again one of surjectivity (as injectivity is clear), so we may assume $m = m_1 m_2$ with relatively prime $m_j > 1$, and the theorem may be assumed to be known for each m_j. We may also assume m_1 is odd. As in the proof of Theorem 3.1, it suffices to separately study a root of unity $z \in \mathbf{Z}'[\zeta_n][x]/(s_m)$ with $z^{m_1} = 1$ and z of order prime to m_1. We again define $\mathbf{Z}'' = \mathbf{Z}'[1/m_2]$. Our replacement for (3.6) is the isomorphism

$$\mathbf{Z}''[\zeta_n][x]/(s_m) \to \mathbf{Z}''[\zeta_n][x]/(s_{m_1}) \times \prod_{d|m_2, d>1} \mathbf{Z}''[\zeta_{nd}][x]/(x^{m_1}-1) \tag{4.2}$$

defined by $x \mapsto (x, (\zeta_d x)_{d|m_2, d>1})$. To see that this map is an isomorphism, the idea is that $s_m(x) = ((x^{m_1})^{m_2}-1)/(x-1)$ with $y^{m_2}-1$ étale over $\mathbf{Z}''$. More precisely, we claim that passing to the mod s_m quotient on the isomorphism (3.6) yields (4.2). To see what is happening on the target ring, consider the factorization $s_m(x) = s_{m_1}(x) \cdot \prod_{\zeta^{m_2}=1, \zeta \neq 1} (x^{m_1} - \zeta)$ in $\mathbf{Z}''[\zeta_{m_2}][x]$. The factors pairwise generate 1, since m_2 is a unit in $\mathbf{Z}''$ and $x^{m_1} - \zeta$ and $x^{m_1}-1$ generate 1 for each $\zeta \neq 1$ (with $s_{m_1} | (x^{m_1}-1)$). Combining this with the fact that $s_m(\zeta_d x)$ is divisible by $x^{m_1}-1$ for $d | m_2$ with $d \neq 1$, we obtain the desired identification of the right side of (4.2) with a quotient of the right side of (3.6), so (4.2) is indeed an isomorphism.

To describe z, we consider its components in the factor rings on the right side of (4.2). We can describe the roots of unity in the first factor-ring via induction for m_1, and for the other factors we can use Theorem 3.1. The arguments with the σ_a's in the proof of Theorem 3.1 exploited the inductive hypothesis for m_2. These arguments carry over essentially unchanged to our present situation once we check that the subring in $\mathbf{Z}'[\zeta_n][x]/(s_m)$ consisting of invariant-elements under all operators $x \mapsto x^a$ (for $a \in (\mathbf{Z}/m)^\times$ with $a \equiv 1 \bmod m_2$) is generated over $\mathbf{Z}'[\zeta_n]$ by $y = x^{m_1}$. Since $(m_2-1)m_1 < m_1 m_2 - 1$ (as $m_1 > 1$), the distinct powers $1, x^{m_1}, \dots, x^{(m_2-1)m_1}$ of x^{m_1} constitute a $\mathbf{Z}'[\zeta_n]$-module direct summand of $\mathbf{Z}'[\zeta_n][x]/(s_m)$; thus, it suffices to show that the subring of invariants after extending scalars to $\mathbf{Q}$ is generated over $\mathbf{Q}(\zeta_n)$ by y. The factor rings of $\mathbf{Q}(\zeta_n)[x]/(s_m)$ are $\mathbf{Q}[\zeta_{nd}]$ for $d = d_1 d_2 | m = m_1 m_2$ with $d \neq 1$, and $x \mapsto x^a$ goes over to the automorphism fixing nd_2th roots of unity and raising d_1th roots of unity to the ath power. Thus, the invariant subfield in each such factor-field is $\mathbf{Q}[\zeta_{nd_2}]$, with ζ_{d_2} a power of the primitive d_2th root of unit $\zeta_d^{m_1}$. This yields the desired subring of invariants (generated by x^{m_1}), completing the proof of Theorem 1.1.

References

[H] G. Higman, *The units of group rings*, Proc. London Math Soc. (2) **46**, 1940, pp. 231–248.
[S] J-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.
[W] L. Washington, *Cyclotomic Fields* 2nd ed., Springer-Verlag, 1997.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: bdconrad@umich.edu