UNRAMIFIED ABELIAN EXTENSIONS OF GALOIS COVERS

Michael D. Fried and Helmut Völklein, U of Florida*

Abstract: We consider a ramified Galois cover $\varphi : \hat{X} \to \mathcal{P}^1_x$ of the Riemann sphere $\mathcal{P}^1_x$, with monodromy group G. The monodromy group over $\mathcal{P}^1_x$ of the maximal unramified abelian exponent n cover of $\hat{X}$ is an extension ${}_n\tilde{G}$ of G by the group $(Z/nZ)^{2g}$, where g is the genus of $\hat{X}$. Denote the set of linear equivalence classes of divisors of degree k on $\hat{X}$ by $\mathrm{Pic}^k(\hat{X}) = \mathrm{Pic}^k$. This is equipped with a natural G action. We show that the equivalence class of the extension ${}_n\tilde{G} \to G$ is determined by the element of $H^1(G, \mathrm{Pic}^0)$ representing Pic^1 (§2.2). From this we give an effective criterion (involving the Schur multiplier of G) to decide when this group extension splits for all n (§4.2). In particular we easily produce examples from this of cases where $\hat{X}$ has G invariant divisor classes of degree 1, but no G invariant divisor of degree 1 (§5.1).
The extension ${}_n\tilde{G} \to G$ naturally factors into a sequence ${}_n\tilde{G} \to H \to G$ where H is the smallest quotient of ${}_n\tilde{G}$ giving a *frattini cover* (§1.1) that fits between ${}_n\tilde{G}$ and G. Extension of the main result of §4.2 would consider all maximal quotients M of ${}_n\tilde{G}$ such that $M \to G$ splits. We note that the sequence including such an M factors through H, and by example we demonstrate that such maximal quotients M may not be unique (§5.2).

INTRODUCTION: We consider a ramified Galois cover $\varphi : \hat{X} \to \mathcal{P}^1_x$ of the Riemann sphere $\mathcal{P}^1_x$, with monodromy group G. Choose an integer $n > 1$. Let $\hat{X}_n$ be the maximal unramified abelian exponent n cover of $\hat{X}$. The monodromy group V_n of this cover is isomorphic to $(Z/nZ)^{2g}$, where g is the genus of $\hat{X}$. Composing with φ we get a Galois cover $\hat{X}_n \to \mathcal{P}^1_x$, whose monodromy group is an extension of G by V_n:

$$(*) \qquad V_n \to {}_n\tilde{G} \to G.$$

Our main goal is to study this group extension. We introduce the notion of "unramified cover" for groups in §1.2. This we use to give a purely group-theoretic construction of the extension (*). To illustrate the analogy between our group-theoretic notion of "unramified cover" and the (already established) notion of "frattini cover," we recall the basic theory of frattini covers. We give a fairly general situation in Lemma 1.2 that implies that the universal exponent n frattini cover with abelian kernel is a quotient of ${}_n\tilde{G}$. This lemma isn't crucial for the rest of the paper, but it is included for future reference and for motivation for the consideration of maximal quotients of ${}_n\tilde{G}$ in §5.2.

AMS Subject classification: 12F05, 14H40, 14D20, 14E20,

Keywords: Extensions of $C(x)$; Riemann's existence theorem; Jacobian varieties and theta functions; modular representations.
*Supported by NSF grant DMS–8702150

For the main story of the paper we embed $\hat{X}$ into its Jacobian, which we identify with the group Pic^0 of divisor classes of degree 0 of $\hat{X}$. (As is well known this embedding is not canonical, but requires a choice of divisor class of degree 1). This yields a realization of $\hat{X}_n$ as the inverse image of this embedded curve under the map $\mathrm{Pic}^0 \to \mathrm{Pic}^0$, by $u \mapsto nu$. This leads to an identification of the kernel V_n from (*) with the group of n-division points of Pic^0, compatible with the natural G module structure on these (abelian) groups. We call this G module V_n the *Hurwitz module* (since its dimension is given by the Riemann-Hurwitz formula). In §3.1, using the classical duality theory of abelian varieties, we show that this module is self-dual (this isn't obvious from the group-theoretic definition in §1.2). Denote the group of all divisor classes of $\hat{X}$, with natural G-action, by Pic. Theorem 2.3 shows how the equivalence class of the group extension (*) is determined by the element of the cohomology group $H^1(G, \mathrm{Pic}^0)$ that defines the G module extension of Pic over Pic^0. In particular, the extension (*) splits for all n if and only if there is a G-invariant divisor class of degree 1 (Corollary 2.5).

It is easy to see that there can be a G-invariant *divisor* of degree 1 only if the group G is metacyclic (§3.2). But, the question of when there is a G-invariant *divisor class* of degree 1 is much more intricate. Using the self-duality of the Hurwitz module, we give a fairly explicit answer to this question in the Main Theorem of §4.2. Roughly speaking, it says that the splitting of all unramified abelian extensions of G is determined by the Schur multiplier of G (i.e., by the *central* extensions). This is a sufficiently practical result for us to illustrate it by examples in §5.1. A natural extension of this topic would be to consider quotients M of ${}_n\tilde{G}$ that factor through G, and for which $M \to G$ is split. In §5.2 we note that if M is a maximal such quotient, then it actually factors through the minimal frattini quotient H of ${}_n\tilde{G}$ (as in §1.1). We conclude the paper with examples that show that such an M is not "the" maximal (i.e., unique) quotient with this splitting property.

Acknowledgements: Conversations with Walter Feit, Roger Howe and John Thompson had a great deal to do with the first author's interest in developing this subject. An appreciable debt is owed to Armand Brumer who had independently understood some of the points of §2 and discussed this with the first author—who may be a little remiss in making precise this debt. Sybilla Beckman [Be] has independently considered the foundational exact sequence (*).

§1. GROUP-THEORETIC PRELIMINARIES

Let G be a finite group with generators $\sigma_1, \ldots, \sigma_r$ satisfying $\sigma_1 \cdots \sigma_r = 1$. Let F_r be the free group on the generators $\bar{\sigma}_1, \ldots, \bar{\sigma}_r$ and let $\pi : F_r \to G$ be the homomorphism that sends $\bar{\sigma}_i$ to σ_i. Let Γ be a class of finite groups closed under isomorphisms, direct products and subgroups.

§1.1. FRATTINI COVERS: A *frattini cover* of G is a finite group H together with a surjective homomorphism $f : H \to G$ whose kernel lies in the frattini subgroup of H. Equivalently, f is surjective, but does not remain surjective when restricted to any proper subgroup of H. We call f a *frattini* Γ-*cover* if the kernel of f belongs to Γ. Clearly, each frattini Γ-cover of G is equivalent to one of the form $f : F_r/N \to G$ with f induced by π (where N is a normal subgroup of F_r contained in $\ker(\pi)$). Call such an f a *standard* frattini Γ-cover, and consider the system of all homomorphisms $\alpha : Q_1 \to Q_2$, where $f_i : Q_i \to G$ is a standard frattini Γ-cover, $i = 1, 2$, and $f_2 \circ \alpha = f_1$. It is readily checked that this is an inverse system; the projective limit of this inverse system is called the *universal frattini* Γ-*cover* of G. We denote this profinite group by $\mathrm{ufc}_\Gamma(G)$. It is easy to extend the notion of frattini cover to the category of profinite groups and to consider the obvious universal property of $\mathrm{ufc}_\Gamma(G)$ [FrJ; §20.7]. These universal frattini covers were first considered in [EF] and [CKK].

If Γ is the class of all finite groups (resp., of all finite p-groups) we write $\tilde{G}$ (resp., ${}_p\tilde{G}$) for $\mathrm{ufc}_\Gamma(G)$ and call it the universal frattini cover of G (resp., the universal p-frattini cover of G). It is known that $\widetilde{G}$ is a projective profinite group. Thus the kernel of ${}_p\widetilde{G} \to G$ is a free pro-p-group [FrJ; §20.7].

If Γ is the class of all finite abelian groups whose exponent divides n, we write $\mathrm{ufc}_n(G)$ for $\mathrm{ufc}_\Gamma(G)$ and call it the universal exponent n abelian frattini cover of G. The frattini covering property implies that $\mathrm{ufc}_n(G)$ is generated by r elements (as a topological group). Since the kernel of the map $\mathrm{ufc}_n(G) \to G$ is of index $|G|$, it is also finitely generated (as a topological group); but this kernel is abelian and has exponent dividing n, hence is a finite group. Thus $\mathrm{ufc}_n(G)$ is actually a finite extension of G. This has been studied in [Ga] and [GS] in the case that n is a prime.

§1.2. UNRAMIFIED COVERS: Continue the earlier notation where $\sigma_1, \ldots, \sigma_r$ are generators of G satisfying $\sigma_1 \cdots \sigma_r = 1$. Define an *unramified* cover of G relative to $\sigma_1, \ldots, \sigma_r$ to be a finite group H together with a homomorphism $f : H \to G$ such that $H = \langle \tau_1, \ldots, \tau_r \rangle$ with $\tau_1 \cdots \tau_r = 1$, $f(\tau_i) = \sigma_i$ and $\mathrm{ord}(\tau_i) = \mathrm{ord}(\sigma_i)$, $i = 1, \ldots, r$. Call such an f an *unramified* Γ-*cover* if the kernel of f belongs to Γ. (Usually we drop the phrase "relative to $\sigma_1, \ldots, \sigma_r$" when we have fixed the set $\{\sigma_1, \ldots, \sigma_r\}$ of generators of G).

We proceed as in §1.1. Again, each unramified Γ-cover of G is equivalent to one of the form $F_r/N \to G$, and these unramified Γ-covers $F_r/N \to G$ again form an inverse system (which is clear from the next paragraph). The projective limit of this inverse system is now called the *universal unramified* Γ-*cover of* G (relative to $\sigma_1, \ldots, \sigma_r$). We denote it by $\mathrm{uuc}_\Gamma(G; \sigma_1, \ldots, \sigma_r)$, or for short, $\mathrm{uuc}_\Gamma(G)$. Again one would have to extend the notion of unramified cover to the category of profinite groups in order to state the (obvious) universal property of $\mathrm{uuc}_\Gamma(G)$.

Let N_0 be the normal subgroup of F_r generated by

$$\bar{\sigma}_1 \cdots \bar{\sigma}_r \qquad \text{and by} \qquad \bar{\sigma}_i^{\mathrm{ord}(\sigma_i)},\ i = 1, \ldots, r.$$

Clearly, a finite group extension $f : H \to G$ is an unramified cover if and only if the map $F_r/N_0 \to G$ (induced by π) factors through f. This implies that the universal unramified cover $\mathrm{uuc}(G)$ (by which we mean $\mathrm{uuc}_\Gamma(G)$, with Γ the class of all finite groups) is the profinite completion of F_r/N_0.

If Γ is the class of all finite abelian groups (resp., finite abelian p-groups), we write $\mathrm{uuc}_{ab}(G)$ (resp., $\mathrm{uuc}_{(p)}(G)$) for $\mathrm{uuc}_\Gamma(G)$ and call it the universal unramified abelian cover (resp., universal unramified abelian p-cover) of G. Let $R = \ker(\pi)$, let R' be the commutator subgroup of R and let N be the subgroup of F_r generated by R' and by N_0. Then $\mathrm{uuc}_{ab}(G)$ is the profinite completion of F_r/N.

If Γ is the class of all finite abelian groups whose exponent divides n, we write $\mathrm{uuc}_n(G)$ for $\mathrm{uuc}_\Gamma(G)$, and call it the universal abelian unramified exponent n cover of G. Let N_n be the subgroup of F_r generated by R', R^n and N_0. Then clearly $\mathrm{uuc}_n(G) \cong F_r/N_n$, a finite group.

Reminder 1.1: *Riemann's existence theorem*: There is a Galois cover $\varphi : \hat{X} \to \mathcal{P}^1_x$ with monodromy group isomorphic to G and with $\sigma_1, \dots, \sigma_r$ a description of its branch cycles [Gr]. Of course, G is also isomorphic to the Galois group of $C(\hat{X})$ over $C(x)$, but the isomorphism isn't canonical. Now consider any cover $\bar{X} \to \hat{X}$ such that the induced cover $\delta : \bar{X} \to \mathcal{P}^1_x$ is Galois, with monodromy group H. We can choose a description $\tau_1, \dots, \tau_s$ of the branch cycles of δ such that the induced homomorphism $f : H \to G$ takes τ_i to σ_i, $i = 1, \dots, r$, and such that there are points $x_1, \dots, x_s$ on $\mathcal{P}^1_x$ with the following properties: The branch points of φ (resp., δ) are among $x_1, \dots, x_r$ (resp., $x_1, \dots, x_s$); and the ramification index of φ (resp., δ) at x_i is the order of σ_i (resp., τ_i). Thus, if the cover $\bar{X} \to \hat{X}$ is unramified in the topological sense (equivalently, the extension $C(\bar{X})/C(\hat{X})$ is unramified in the field-theoretic sense) then $f : H \to G$ is an unramified cover in the sense defined above. Note that we may choose an isomorphism of H with the Galois group of $C(\bar{X})/C(x)$, similarly as the above isomorphism $G \cong G(C(\hat{X})/C(x))$. Furthermore, in this case, $f : H \to G$ corresponds to the restriction map between these Galois groups. Conversely, given an unramified cover $f : H \to G$, Riemann's existence theorem produces a cover $\bar{X} \to \hat{X} \to \mathcal{P}^1_x$ as above, and the same argument shows that $C(\bar{X})$ is unramified over $C(\hat{X})$. □

It follows that the maximal unramified Γ-extension of $C(\hat{X})$ is Galois over $C(x)$ with Galois group isomorphic to $\mathrm{uuc}_\Gamma(G)$. Thus the kernel of the map $\mathrm{uuc}(G) \to G$ is isomorphic to the algebraic fundamental group of $C(\bar{X})$ [Gr]. In particular, the kernel of the map $\mathrm{uuc}_n(G) \to G$ is isomorphic $(Z/nZ)^{2g}$, where g is the genus of $\hat{X}$, given by the Riemann-Hurwitz formula:

$$2(|G| + g - 1) = |G| \sum_{i=1}^{r} (1 - (\mathrm{ord}(\sigma_i))^{-1}).$$

The next lemma is not essential for the remainder of the paper, but it does describe a situation that comes up in practice that will be used for examples in subsequent papers. Consider an r-tuple $(\rho_1, \dots, \rho_r)$ of elements from a group G such that the entries generate G and the product in order of the entries is 1. Then the r-tuple

$$(\rho_1, ..., \rho_r)^{Q_i} = (\rho_1, \dots, \rho_{i-1}, \rho_{i+1}, \rho_{i+1}^{-1}\rho_i\rho_{i+1}, \dots, \rho_r),\ i = 1, \dots, r-1$$

also has these same properties. The set of r-tuples given by iterations of the operations $\{Q_1, \dots, Q_{r-1}\}$ is called an orbit of $(\rho_1, \dots, \rho_r)$ under the action of the *Hurwitz monodromy group* H_r. It is so named for there being such a combinatorial group and for the significance of this particular action to the production of moduli spaces (cf. [Fr] and [Ma]). But its use in the next lemma will be quite elementary.

Lemma 1.2: *Suppose r is even. Assume also that the orbit of $(\sigma_1, \dots, \sigma_r)$ under the action of H_r contains an element that is conjugate under G (or, more generally, under an automorphism of G) to an r-tuple $(\rho_1, \dots, \rho_r)$ with $\rho_{2i-1} = \rho_{2i}^{-1}$, $i = 1, \dots, r/2$. Then for all positive integers n prime to $\mathrm{lcm}(\mathrm{ord}(\sigma_1), \dots, \mathrm{ord}(\sigma_r))$, the frattini cover $\mathrm{ufc}_n(G) \to G$ is unramified relative to $\sigma_1, \dots, \sigma_r$.*

Proof: Set $H = \mathrm{ufc}_n(G)$ and let $f : H \to G$ be the canonical map. We must show that $\sigma_1, \dots, \sigma_r$ lift to generators $\tau_1, \dots, \tau_r$ of H with this property:

1.1) $\tau_1 \cdots \tau_r = 1$ and $\mathrm{ord}(\tau_i) = \mathrm{ord}(\sigma_i)$, $i = 1, \dots, r$.

Property 1.1) is preserved if we replace $\sigma_1, \dots, \sigma_r$ by the image of this collection under an operation from H_r. Therefore, from the statement about the action of H_r, we may assume $\sigma_1 = \rho_1, \dots, \sigma_r = \rho_r$. Now choose τ_{2i} to be any element of H mapping to σ_{2i}, $i = 1, \dots, r/2$. The kernel of f is of exponent n and n is prime to the order of σ_{2i}. Therefore, if we replace τ_{2i} by a suitable power we may assume that $\mathrm{ord}(\tau_{2i}) = \mathrm{ord}(\sigma_{2i})$. Setting $\tau_{2i-1} = \tau_{2i}^{-1}$ guarantees 1.1), and $f(\tau_i) = \sigma_i$ for all i. Finally, since f is a frattini cover, the latter condition implies $H = \langle \tau_1, \dots, \tau_r \rangle$. □

Remark: *Generalization of the condition on the ρ_i's.* For example, one could replace the hypothesis of Lemma 1.2 by the condition that there is a partitioning of the elements $\rho_1, \dots, \rho_r$ such that the elements in each block of the partition have product equal to 1 and each of them in the block is equal to a power of a single element in the block. Another possibility, if G can be generated by two elements, say, ρ_1 and ρ_2, would be to prescribe how the other ρ_i's are represented as words in ρ_1 and ρ_2, etc. □

§2. UNRAMIFIED COVERS AND THE JACOBIAN

Again we fix a finite group G with generators $\sigma_1, \dots, \sigma_r$ satisfying $\sigma_1 \cdots \sigma_r = 1$. Let $\varphi : \hat{X} \to \mathcal{P}^1_x$ be a Galois cover with monodromy group G and $\sigma_1, \dots, \sigma_r$ a description of its branch cycles. We let g denote the genus of $\hat{X}$. As in Remark 1.1, choose an isomorphism of G with the group $\mathrm{Aut}(\hat{X}, \varphi)$ of automorphisms of the cover φ. Through this isomorphism, we identify G from now on with $\mathrm{Aut}(\hat{X}, \varphi)$.

§2.1. HURWITZ MODULES AND SEQUENCES DEFINED BY Pic**:** This subsection exhibits relations between the Jacobian of $\hat{X}$ and the group extension

$$V_n \to \mathrm{uuc}_n(G) \to G. \tag{2.1}$$

Here $n > 1$ is an integer and V_n is the kernel of the map $\mathrm{uuc}_n(G) \to G$. View V_n as a G module in the natural way: an element $g' \in \mathrm{uuc}_n(G)$ acts by conjugation on V_n, and since V_n is abelian this action is dependent only on the image of g' in G. Call V_n the *Hurwitz module* (corresponding to n; for the data given by G and $\sigma_1, \dots, \sigma_r$). Further, we call extension 2.1) the *Hurwitz extension* when all other data has been named so as to make this unambiguous. Let Pic (resp., Pic^k) denote the set of linear equivalence classes of divisors (resp., of divisors of degree k) on $\hat{X}$ (for any integer k). The abelian groups Pic and Pic^0 are naturally G modules.

Identify Pic^0 with the Jacobian of $\hat{X}$. So, Pic^0 becomes an abelian variety of dimension g on which G acts by complex-analytic automorphisms. Then each Pic^k carries a natural structure of complex manifold (as principal homogeneous space for Pic^0). If $g > 0$ the curve $\hat{X}$ is canonically, G-equivariantly, embedded in Pic^1 by mapping a point $\boldsymbol{p} \in \hat{X}$ to the divisor class of the point.

Let Π denote the group of "affine" transformations $u \mapsto \sigma(u) + w$ of Pic with $\sigma \in G$ and $w \in \mathrm{Pic}$. View G as a subgroup of Π in the natural way to see that Π is the semi-direct product of $\mathcal{T}$ and G where $\mathcal{T}$ is the normal subgroup of translations $T_w : u \mapsto u + w$. We denote this semidirect product by $\mathcal{T} \times^s G$. Pick some $w \in \mathrm{Pic}^1$ and let C denote the translated curve $T_{-w}(\hat{X}) \subset \mathrm{Pic}^0$. Then the subgroup $G_w = (T_w)^{-1} G T_w$ of Π leaves C invariant. Let $\mathrm{Pic}^0(n) = \{u \in \mathrm{Pic}^0 \mid nu = 0\}$ be the group of n-division points of Pic^0, and consider $\mathcal{T}_n = \{T_u : u \in \mathrm{Pic}^0(n)\}$. The inverse image C_n of C under the isogeny $\mu_n : \mathrm{Pic}^0 \to \mathrm{Pic}^0$, given by $u \mapsto nu$, is an unramified Galois cover of C with $\mathcal{T}_n$ as its group of deck transformations (i.e., automorphisms that commute with the map to C). It is a classical result that the curve C_n is connected [Se;]. Since $\mathcal{T}_n \cong (Z/nZ)^{2g}$, the cover $C_n \to C$ (induced by μ_n) is the maximal unramified exponent n abelian cover of C.

The action of multiplication by n on elements of Pic commutes with the action of G. Therefore it induces a group homomorphism $\nu_n : \Pi \to \Pi$ which is the identity on G and sends each $T_w \in \mathcal{T}$ to T_{nw}. Then $\ker(\nu_n) = \mathcal{T}_n$; and the group $H_n = \nu_n^{-1}(G_w)$ is an extension of G by $\mathcal{T}_n$ through the map $f_n : H_n \to G$, $h \mapsto T_w \nu_n(h) (T_w)^{-1}$.

Lemma 2.1: *The map $f_n : H_n \to G$ is a universal unramified exponent n abelian cover.*

Proof: The composition of maps

$$C_n \xrightarrow{\mu_n} C \xrightarrow{T_w} \hat{X}$$

gives a cover $\delta_n : C_n \to \hat{X}$ with $\mathcal{T}_n$ as its group of deck transformations. Since $\mathcal{T}_n \subseteq H_n$, the cover $\varphi_n : C_n \to C_n/H_n$ factors through δ_n by some cover ϵ:

$$C_n \xrightarrow{\delta_n} \hat{X} \xrightarrow{\epsilon} C_n/H_n.$$

Now δ_n induces a surjection $H_n \to \mathrm{Aut}(\hat{X}, \epsilon)$. from the above it is clear that this homomorphism is exactly the map $f_n : H_n \to G$. Thus $G = \mathrm{Aut}(\hat{X}, \epsilon)$. This means that the cover ϵ is equivalent to our original cover $\varphi : \hat{X} \to \mathcal{P}^1_x$. Since δ_n is the maximal unramified abelian exponent n-cover of $\hat{X}$, the claim follows using Reminder 1.1. □

Corollary 2.2: *The Hurwitz module V_n is isomorphic to the module $\mathrm{Pic}^0(n)$ of n-division points of Pic^0 (with natural G action).*

§**2.2. THE IMAGE OF** $[\hat{X}]$ **IN** $H^2(G, (Z/nZ)^{2g})$**:** Our main result shows how the group extension 2.1) is determined by the G module extension of Pic over Pic^0. In particular, Pic splits over Pic^0 as a G module (equivalently, Pic^1 is isomorphic to Pic^0 as a G-variety) if and only if the group extension 2.1) splits for all n. In §4 we characterize when this occurs in terms of pure group theory. To formulate the result, consider the exact sequences

$$0 \to \mathrm{Pic}^0(n) \to \mathrm{Pic}^0 \xrightarrow{\mu_n} \mathrm{Pic}^0 \to 0; \text{ and} \tag{2.2}$$

$$0 \to \mathrm{Pic}^0 \to \mathrm{Pic} \xrightarrow{\deg} Z \to 0 \tag{2.3}$$

of G modules. Extension 2.3) defines an element of $H^1(G, \mathrm{Pic}^0) \cong \mathrm{Ext}^1_G(Z, \mathrm{Pic}^0)$, which we denote by $[\hat{X}]$. It is represented by the cocycle $\sigma \mapsto w - \sigma(w)$ with $w \in \mathrm{Pic}^1$ as above.

Theorem 2.3: *Let α be the image of $[\hat{X}]$ under the connecting map $H^1(G, \mathrm{Pic}^0) \to H^2(G, \mathrm{Pic}^0(n))$ that arises in the long cohomology sequence associated to 2.2), and let*

$$\mathrm{Pic}^0(n) \to H \xrightarrow{f} G$$

be a group extension in the equivalence class defined by α. Then the map $f : H \to G$ is a universal unramified exponent n abelian cover of G.

For the proof we need an elementary fact about group cohomology which is easily deduced from [N; p. 235]. We state this as a separate lemma about an exact sequence

$$0 \to N \to M \to K \to 0 \tag{2.4}$$

of G modules.

Lemma 2.4: *In sequence 2.4) let*

$$N \times^s G \to M \times^s G \xrightarrow{\nu} K \times^s G$$

be the induced sequence of semi-direct products. Let c be a 1-cocycle of G in K; it defines the complement

$$D = \{(c(\sigma), \sigma) \mid \sigma \in G\}$$

of K in the semi-direct product $K \times^s G$. Let $\psi : \nu^{-1}(D) \to G$ be the restriction of $\mathrm{pr} \circ \nu$, where $\mathrm{pr} : K \times^s G \to G$ is the canonical projection. Then the element of $H^2(G, N)$ that corresponds to the class of the group extension

$$N \to \nu^{-1}(D) \xrightarrow{\psi} G$$

is the image of the class of c under the connecting map $H^1(G, K) \to H^2(G, N)$ that arises in the long cohomology sequence associated to 2.4).

Proof of Theorem 2.3: Identify Pic canonically with $\mathcal{T}$ through the G-equivariant isomorphism that sends u to T_u. Then the element $-[\hat{X}]$ is identified with the class of the cocycle $\sigma \mapsto T_w^{-1} \sigma T_w \sigma^{-1}$. This cocycle defines

$$G_w = T_w^{-1} G T_w = \{(T_w^{-1} \sigma T_w \sigma^{-1}, \sigma) \mid \sigma \in G\}$$

as a complement to $\mathcal{T}^0 = \{T_u : u \in \mathrm{Pic}^0\}$ in the semi-direct product $\mathcal{T}^0 \times^s G$. Thus by Lemma 2.4, the image $-\alpha$ of $-[\hat{X}]$ in $H^2(G, \mathrm{Pic}^0(n))$ is identified with the element of $H^2(G, \mathcal{T}_n)$ corresponding to the class of the group extension

$$\mathcal{T}_n \to H_n \xrightarrow{f_n} G$$

from Lemma 2.1. Replace the inclusion map $\mathcal{T}_n \to H_n$ in this sequence by the map $T_u \mapsto T_u^{-1}$ to obtain a group extension in the equivalence class corresponding to α. But by Lemma 2.1, the map $f_n : H_n \to G$ in this group extension is a universal unramified exponent n abelian cover of G. Hence the claim. □

Corollary 2.5: *The following are equivalent:*

a) Pic *splits over* Pic^0 *as a* G *module;*
b) G *has a fixed point on* Pic^1*;*
c) *the group extension* 2.1) *splits for all* n*;*
d) 2.1) *splits for all* $n = p^k$ *with* $k = 1, 2, \ldots$ *and* p *a prime divisor of* $|G|$*;*
e) *each (finite) unramified abelian cover of* G *is a split extension of* G*; and*
f) *The universal unramified abelian cover* $\mathrm{uuc}_{ab}(G) \to G$ *is a split extension of* G*.*

Proof: a) and b) are trivially equivalent, and they imply c) by Theorem 2.3. Also c) and d) are clearly equivalent by Zassenhaus' Theorem [Hu; §18.1]. Furthermore it is immediate that f) implies e) and e) implies c). We now show that b) implies f). Assume b). Choose $w \in \mathrm{Pic}^1$ to be a fixed point of G to see that $G_w = G$ and therefore $H_n = \mathcal{T}_n \times^s G$. From Lemma 2.1 conclude the following: if we arrange the groups H_n naturally in an inverse system (with maps $H_n \to H_m$, for m a divisor of n, given by $\nu_{n/m}$), then $\mathrm{uuc}_{ab}(G)$ is isomorphic to the projective limit of this inverse system; and in the present situation, the natural splittings $G \to H_n$ glue together to yield a splitting of the projective limit. This proves (f).
It remains to prove that c) implies a). First we show that $H^1(G, \mathrm{Pic}^0)$ is a finitely generated abelian group. (Since the order of each element divides the order of $|G|$, it is in fact a finite group.) By Abel's theorem, we know there is an exact sequence of abelian groups

$$0 \to \Lambda \to C^g \to \mathrm{Pic}^0 \to 0 \qquad 2.5)$$

where Λ is a lattice (= free abelian group of rank $2g$) in C^g. The action of G can be lifted to a linear action on C^g leaving Λ invariant, so that 2.5) becomes an exact sequence of G modules. The associated long cohomology sequence yields $H^1(G, \mathrm{Pic}^0) \cong H^2(G, \Lambda)$, since $H^i(G, C^g) = 0$ for all $i > 0$ [HS, §16.7]. But since Λ is finitely generated, so is $H^2(G, \Lambda)$ a finitely generated abelian group, and therefore so is $H^1(G, \mathrm{Pic}^0)$.
Now assume c). Then by Theorem 2.3, the element $[\hat{X}]$ is in the kernel of the connecting map $H^1(G, \mathrm{Pic}^0) \to H^2(G, \mathrm{Pic}^0(n))$ for all n. Hence $[\hat{X}]$ is in the image of the map $H^1(G, \mathrm{Pic}^0) \to H^1(G, \mathrm{Pic}^0)$ induced by μ_n. But this induced map is just multiplication by n. Therefore $[\hat{X}]$ is an infinitely divisible element of the finitely generated abelian group $H^1(G, \mathrm{Pic}^0)$. This forces $[\hat{X}] = 0$, which proves a). □

Remarks: *Extension of Corollary 2.5*: We have 3 such remarks.
a) *Replacing* $\mathcal{P}^1_x$ *by a general curve.* In the above it is irrelevant that φ is a cover of $\mathcal{P}^1_x$. We could replace $\mathcal{P}^1_x$ by any curve Y, with the appropriate redefinition of $\mathrm{uuc}_n(G)$ and $\mathrm{uuc}_{ab}(G)$.
b) *A result for each prime* p. The proof of the Corollary can be refined to show that for each prime p the following are equivalent:

i) the order of $[\hat{X}]$ is prime to p;
ii) G fixes a point of Pic^m for some m prime to p;
iii) the group extension 2.1) splits for all $n = p^k$ with $k = 1, 2, \ldots$;
iv) each (finite) unramified abelian p-extension of G splits; and
v) the universal unramified abelian p-cover $\mathrm{uuc}_{(p)}(G) \to G$ is a split extension of G.

c) *Explicit identification of the extension involving* Λ. Let β be the image of $\hat{X}$ under the isomorphism $H^1(G, \mathrm{Pic}^0) \to H^2(G, \Lambda)$ occurring in the proof of 2.5, and let

$$\Lambda \to \bar{G} \to G$$

be a group extension in the class of β. Then $\bar{G}$ is isomorphic to the group F_r/N considered in §1.2. In particular, its profinite completion is $\mathrm{uuc}_{ab}(G)$. The proof is similar to that of Theorem 2.3, working with the sequence 2.5) instead of 2.2). □

§3. SELFDUALITY AND G-INVARIANT DIVISOR CLASSES

Here we hardly touch the details for displaying the module structure of V_n. But from the last section we know that the "frattini module" $\ker(\mathrm{ufc}_n(G) \to G)$ is a quotient of V_n under the hypothesis of Lemma 1.2.

§3.1. SELFDUALITY OF V_n: Our main observation is that V_n is G-dual to itself. This will be an essential ingredient in the proof of Theorem 4.3 below.

Proposition 3.1: *The Hurwitz module V_n is selfdual as a $Z/nZ[G]$ module.*

Proof: As at the beginning of §2.1 consider the curve $C \subset \mathrm{Pic}^0$ equal to the translated curve $T_{-w}(\hat{X})$ with w any point in Pic^1. Taking $g-1$ times the sum of C with itself (as a subset of the group Pic^0) yields a divisor—actually an irreducible subvariety of codimension 1 of Pic^0. This is a translate of the classical Θ divisor as considered in [L,1; Ch. VI, Thm. 3]. Also Θ is fixed by the group $T_w^{-1}GT_w$. Thus for each $\sigma \in G$ there is a translation T_v ($v \in \mathrm{Pic}^0$) such that $\sigma(\Theta) = T_v(\Theta)$.
Now consider the sequence 2.5) of G modules. To each divisor on Pic^0 there is associated a *Riemann form* on (C^g, Λ) [L,2; Ch. VI]. Also, the Riemann form E associated to any translate of Θ (e.g., to $T_v(\Theta)$) is the same as the one associated to Θ [L,2; Ch. VI, Lemma 5.1]. It follows that G leaves the Riemann form E invariant.
By [L,1; Ch. VI, Th. 3] and [L,2; Ch. VI, Thm. 5.3] the Riemann form E has all of its elementary divisors equal to 1. This means that the restriction of E to Λ is an alternating Z-valued form B such that the matrix describing B relative to any basis of Λ has determinant 1. By the above, B is invariant under G:

$$B(\ell_1, \ell_2) = B(\sigma(\ell_1), \sigma(\ell_2)) \qquad 3.1)$$

for each $\ell_1, \ell_2 \in \Lambda$ and $\sigma \in G$. Indeed, as further explanation, the value of the left side of 3.1) can be regarded as an oriented count of the number of points of intersection of the natural parallelogram in C^g with sides given by the vectors ℓ_1 and ℓ_2 with the pullback of Θ to C^g (this has an infinite number of components) [Gu; p. 136]. Similarly for the right side with ℓ_1 and ℓ_2 replaced by $\sigma(\ell_1)$ and $\sigma(\ell_2)$. But it is clear from the natural action of σ on all of the objects that the left side is also equal to the oriented intersection of the parallelogram given by $\sigma(\ell_1)$ and $\sigma(\ell_2)$ with $\sigma(\Theta)$. Since this last is just a translate of Θ, the result derives from the invariance of this number under translation by the Θ divisor.
Thus 3.1) shows that B induces a G-invariant Z/nZ-valued form on $\Lambda/n\Lambda$ that can be described by a matrix of determinant 1. This means that $\Lambda/n\Lambda$ is selfdual as a $Z/nZ[G]$ module. But $\Lambda/n\Lambda \cong n^{-1}\Lambda/\Lambda \cong \mathrm{Pic}^0(n) \cong V_n$ by Corollary 2.2. □

§3.2. METACYCLIC GROUPS AND G-INVARIANT DIVISORS: In this subsection, we complete a part of the characterization for satisfaction of the equivalent conditions of Corollary 2.5. That is, the first step in characterizing the existence of G-invariant divisor classes in Pic^1 is to clarify the existence of G-invariant divisors. Let Div (resp., Div^k) denote the group (resp., set) of divisors (resp., divisors of degree k) on $\hat{X}$.

Lemma 3.2: *There exists a G-invariant divisor on $\hat{X}$ of degree k if and only if k is a multiple of $d = \gcd([G:\langle\sigma_1\rangle],\dots,[G:\langle\sigma_r\rangle])$.*

Proof: A divisor $D \in \mathrm{Div}^k$ is G-invariant if and only if for each G-orbit O on $\hat{X}$ all points from the orbit occur with the same coefficient n_O in D. In this case, $k = \deg(D) = \sum n_O \ell_O$, where ℓ_O is the length of the orbit O. But the orbits of G on $\hat{X}$ are all regular orbits except those lying over the branch points of φ, and the points lying over a branchpoint with branch cycle σ_i form an orbit of length $[G:\langle\sigma_i\rangle]$. This proves the "only if" part of the lemma. The "if" part follows by forming a divisor of degree k which is in the group generated by the divisors lying over the branch points of φ. □

Remark: It follows that there is always a G-invariant divisor of degree $2(g-1)$: by the Riemann-Hurwitz formula we have

$$2(g-1) = -2|G| + \sum_{i=1}^{r} [G:\langle\sigma_i\rangle](\mathrm{ord}(\sigma_i) - 1)$$

hence d divides $2(g-1)$. □

Corollary 3.3: *The order of $[\hat{X}]$ divides d, and thus the extension $\mathrm{uuc}_n(G) \to G$ splits for all n that are prime to d.*

Proof: By Lemma 3.2, G has a fixed point on Pic^d. This implies that $d \cdot [\hat{X}] = 0$. This proves the first assertion. Since $H^2(G, \mathrm{Pic}^0(n))$ has exponent dividing n, the second assertion follows from Theorem 2.3. □

Corollary 3.4: *There is a G-invariant divisor of degree 1 if and only if each Sylow subgroup of G is contained in some $\langle\sigma_i\rangle$. This can only happen if G is metacyclic (i.e., an extension of a cyclic group by a cyclic group).*

Proof: The first assertion follows from Lemma 3.2. A group with all Sylow subgroups cyclic must be metacyclic [Hu; Ch. 4, Th. 3.11]. This gives the second assertion. □

§4. G-INVARIANT DIVISOR CLASSES OF DEGREE 1

From Corollary 3.4 one may expect that the condition that there is a G-invariant divisor *class* of degree 1 will also severely restrict the structure of G. This is indeed so, but the answer is not as simple as for the G-invariant divisors. The natural approach is to look at the following diagram of G modules with exact rows and commutative squares

4.1)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{P} & \longrightarrow & \mathrm{Div}^0 & \longrightarrow & \mathrm{Pic}^0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{P} & \longrightarrow & \mathrm{Div} & \longrightarrow & \mathrm{Pic} & \longrightarrow & 0 \end{array}$$

where $\mathcal{P}$ is the group of principal divisors.

§**4.1. RESULTS ON** $H^k(\mathrm{Div})$**,** $k = 0,\ 1$**:** The two long exact cohomology sequences associated to the rows of 4.1) fit into another diagram with the same properties:

4.2*a*)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(\mathcal{P}) & \longrightarrow & H^0(\mathrm{Div}^0) & \longrightarrow & H^0(\mathrm{Pic}^0) & \longrightarrow & H^1(\mathcal{P}) \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^0(\mathcal{P}) & \longrightarrow & H^0(\mathrm{Div}) & \longrightarrow & H^0(\mathrm{Pic}) & \longrightarrow & H^1(\mathcal{P}) \end{array}$$

4.2*b*)
$$\begin{array}{ccccccccc} & \longrightarrow & H^1(\mathrm{Div}^0) & \longrightarrow & H^1(\mathrm{Pic}^0) & \longrightarrow & H^2(\mathcal{P}) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \dots \\ & \longrightarrow & 0 & \longrightarrow & H^1(\mathrm{Pic}) & \longrightarrow & H^2(\mathcal{P}) & \longrightarrow & \dots \end{array}$$

Since the group G is fixed we have for convenience written $H^0(\mathcal{P})$ instead of $H^0(G, \mathcal{P})$, etc. We will continue to do so for the remainder of this section. Furthermore, d will always be as defined in Lemma 3.2. First we identify a few terms in diagram 4.2). Note that the 0 in 4.2 b) is justified by Part a) of our next lemma.

Lemma 4.1: *The following hold for diagram 4.2):*

a) $H^1(\mathrm{Div}) = 0$;
b) $H^1(\mathrm{Div}^0)$ *is cyclic of order* d*, and it is generated by the class of the cocycle* $\sigma \mapsto D - \sigma(D)$*, for any* $D \in \mathrm{Div}^1$*; and*
c) *the connecting map in the long cohomology sequence associated to the exact sequence of* G *modules*

4.3) $$1 \to C^* \to C(\hat{X})^* \to \mathcal{P} \to 0$$

yields an isomorphism $H^i(\mathcal{P}) \to H^{i+1}(C^*)$*,* $i = 1,\ 2$.

Proof of a): As a G module, Div is isomorphic to the direct sum of certain induced modules $\mathrm{Ind}_H^G(Z)$, one for each orbit of G on $\hat{X}$, where Z is the trivial module and H takes on the values $\{1\}, \langle\sigma_1\rangle, \dots, \langle\sigma_r\rangle$. But by Shapiro's Lemma, $H^1(G, \mathrm{Ind}_H^G(Z)) \cong H^1(H, Z) \cong \mathrm{Hom}(H, Z) = 0$.

Proof of b): Apply a) to the exact cohomology sequence derived from the exact sequence of G modules

$$0 \to \mathrm{Div}^0 \to \mathrm{Div} \xrightarrow{deg} Z \to 0.$$

The result is the exact sequence $H^0(\mathrm{Div}) \to Z \to H^1(\mathrm{Div}^0) \to 0$. The image of the first map is the subgroup of Z generated by d (given in Lemma 3.2). This the first assertion of b). The second assertion follows from the definition of the connecting map.

Proof of c): This follows from Tsen's theorem that $H^i(G, C(\hat{X})^*) = 0$, $i = 1,\ 2,\ 3$. □

Remark: *When* G *has trivial Schur multiplier group.* From c) of Lemma 4.1, if G has trivial *Schur multiplier* $H^2(G, C^*)$, then the map $H^0(\mathrm{Div}) \to H^0(\mathrm{Pic})$ is surjective. In this case, the existence of a G-fixed point on Pic^1 implies the existence of a G-fixed point on Div^1. Corollary 3.4 in turn implies that G is metacyclic. □

Lemma 4.2: *The index $I = [H^0(\mathrm{Div}^0) : H^0(\mathcal{P})]$ is a multiple of the order of each finite abelian group U with the property that the projection $U \times G \to G$ is an unramified cover (relative to $\sigma_1, \ldots, \sigma_r$ as in §1.2).*

Proof: Denote the commutator subgroup of G by G'. For each U with the above property, the abelian group $U \times G/G'$ is generated by elements $\bar{\sigma}_1, \ldots, \bar{\sigma}_r$ with $\bar{\sigma}_1 + \cdots + \bar{\sigma}_r = 0$ and $e_i\bar{\sigma}_i = 0$ with $e_i = \mathrm{ord}(\sigma_i)$, $i = 1, \ldots, r$. Thus $U \times G/G'$ is a quotient of

$$S = (Z/e_1Z \oplus \cdots \oplus Z/e_rZ)/\langle(1, \ldots, 1)\rangle.$$

Therefore $|U||G/G'|$ divides $|S|$. Thus the claim will follow from the following statement:

4.4) $$|S| = I|G/G'|.$$

From 4.3) we get the exact sequence $C(x)^* \to H^0(\mathcal{P}) \to H^1(C^*) \to 0$ upon application of Tsen's theorem and the observation that the fixed field of G in $C(\hat{X})$ is $C(x)$. Since

$$H^1(C^*) = \mathrm{Hom}(G, C^*) \cong G/G',$$

the index J of the image of $C(x)^*$ in $H^0(\mathrm{Div}^0)$ equals $I|G/G'|$. Therefore 4.4) is equivalent to showing that $|S| = J$, which consumes the remainder of the proof.
For each G-orbit O on $\hat{X}$ let $D_O \in \mathrm{Div}$ be the divisor that is the sum of all points in O. We know that $H^0(\mathrm{Div})$ consists of the divisors

$$D = \sum m_O D_O \quad \text{with} \quad \sum \mathrm{m_O|O|} = 0$$

($m_O \in Z$, summation over all G-orbits O on $\hat{X}$). The image of $C(x)^*$ is the subgroup H of $H^0(\mathrm{Div}^0)$ defined by the property that for each O, m_O is a multiple of $e_O = |G|/|O|$ (= the ramification index of any point in the orbit O). Clearly, there are orbits $O_1, \ldots, O_t$ with $e_{O_i} = e_i (= \mathrm{ord}(\sigma_\mathrm{i}))$ for $i = 1, \ldots, t$, and $e_O = 1$ for all other orbits. Thus the subgroup H is the kernel of the map

$$\psi : H^0(\mathrm{Div}^0) \to Z/e_1Z \oplus \cdots \oplus Z/e_tZ$$

that sends $\sum m_O D_O$ to $(m_{O_1}, \ldots, m_{O_t})$. In particular, J is the cardinality of the image of ψ which is clearly

$$\{\Big(\alpha_1, \ldots, \alpha_t\Big) \in Z/e_1Z \oplus \cdots \oplus Z/e_tZ \;\Big|\; \frac{|O_1|}{d}\bar{\alpha}_1 + \cdots + \frac{|O_t|}{d}\bar{\alpha}_t = 0\Big\}$$

where $\bar{\alpha}_i$ denotes the image of α_i in $Z/\bar{e}$ and

$$\bar{e} \stackrel{\mathrm{def}}{=} \frac{|G|}{d} = \mathrm{lcm}(e_1, \ldots, e_t).$$

Note: $\bar{e}$ is the exponent of $Z/e_1Z \oplus \cdots \oplus Z/e_tZ$. Since

$$\gcd\Big(\frac{|O_1|}{d}, \ldots, \frac{|O_t|}{d}\Big) = \gcd\Big(\frac{|G|}{e_1d}, \ldots, \frac{|G|}{e_td}\Big) = 1,$$

conclude that the image of ψ has the same cardinality as S (namely, $e_1 \cdots e_t/\bar{e}$). This proves $|S| = J$, and thereby the lemma. □

Remark: There exists a group U such that actual equality holds in Lemma 4.2, but we do not need this. □

§**4.2.** G**-INVARIANT DIVISOR CLASSES IMPLY CYCLIC SCHUR MULTIPLIERS:** Finally we can now give a precise answer to the question of when the equivalent conditions of Corollary 2.5 hold. The integer d of iv) is given in Lemma 3.2. It is the minimal positive degree of a G-invariant divisor on $\hat{X}$.

Theorem 4.3: *The following are equivalent:*

i) *every (finite) unramified abelian extension of G splits;*
ii) *the canonical map $H^1(\mathcal{P}) \to H^1(\mathrm{Div}^0)$ is an isomorphism;*
iii) *the canonical map $H^1(\mathcal{P}) \to H^1(\mathrm{Div}^0)$ is surjective; and*
iv) *the Schur multiplier group of G is cyclic of order d and each (finite) unramified central extension of G splits.*

Proof: Trivially ii) implies iii). Condition iii) implies that the map $H^1(\mathrm{Div}^0) \to H^1(\mathrm{Pic}^0)$ is zero. But under this map, the class of the cocycle from Lemma 4.1 b) is mapped to $[\hat{X}]$. Hence iii) implies $[\hat{X}] = 0$, which gives i) by Corollary 2.5.

Since the kernel of the map $H^0(\mathrm{Pic}^0) \to H^1(\mathcal{P})$ is isomorphic to $H^0(\mathrm{Div}^0)/H^0(\mathcal{P})$, which is finite by Lemma 4.2, it is finite. By Lemma 4.1 c) the image of this map is isomorphic to a subgroup of the Schur multiplier group of G, and it too is therefore finite. Hence $H^0(\mathrm{Pic}^0)$ is finite and $H^0(\mathrm{Pic}^0) \subset \mathrm{Pic}^0(n)$ for some positive integer n. Take duals with respect to Z/nZ of these G modules. By Proposition 3.1 it follows that $H^0(\mathrm{Pic}^0)$ is also a G module quotient of $\mathrm{Pic}^0(n)$. Corollary 2.2 identifies $\mathrm{Pic}^0(n)$ with V_n, hence $H^0(\mathrm{Pic}^0)$ is also a G-module quotient of V_n. For the following considerations, let K be a submodule of V_n with $V_n/K \cong H^0(\mathrm{Pic}^0)$. Now assume i). This implies that sequence 2.1) splits, i.e., the projection $V_n \times^s G \to G$ is an unramified cover (rel. $\sigma_1, ..., \sigma_r$). Dividing out by K it follows that $H^0(\mathrm{Pic}^0)$ has the property of the group U of Lemma 4.2. Thus $[H^0(\mathrm{Div}^0) : H^0(\mathcal{P})] \geq |H^0(\mathrm{Pic}^0)|$, which means that the image of $H^0(\mathrm{Div}^0)$ in $H^0(\mathrm{Pic}^0)$ exhausts all of $H^0(\mathrm{Pic}^0)$. Again from the long cohomology sequence it follows that the map $H^1(\mathcal{P}) \to H^1(\mathrm{Div}^0)$ is injective. This map, however, is also surjective: the generator of $H^1(\mathrm{Div}^0)$ given in Lemma 4.1 b) maps to $[\hat{X}]$ in $H^1(\mathrm{Pic}^0)$, and $[\hat{X}] = 0$ by Corollary 2.5 (since we are assuming i)).

So we have deduced ii). From the identifications in Lemma 4.1) this also gives the first part of iv). But the second part of iv) holds trivially under hypothesis i). Thus we have shown that i) implies iv).

It remains to show that iv) implies ii). As above we see that iv) implies that the map $H^1(\mathcal{P}) \to H^1(\mathrm{Div}^0)$ is injective. But iv) and Lemma 4.1 imply that these two groups are cyclic of the same order. Therefore the map is an isomorphism: ii) holds. □

§5. EXAMPLES

Theorem 4.3 says roughly that the splitting of all unramified abelian extensions of G is already determined by the *central* extensions. Since a lot is known about central extensions this yields an effective criterion for verifying the validity of i) .

§5.1. CASES OF COVERS WHERE ALL HURWITZ SEQUENCES SPLIT: For an explicit example, consider $G = \mathrm{PSL}_2(p)$ for a prime $p > 3$. Then G is simple. It also has Schur multiplier group equal to $Z/2$ and all of the Sylow subgroups of G except the Sylow 2-subgroups are cyclic [Hu; Chap. V, 25.7]. Furthermore each Sylow 2-subgroup has a cyclic subgroup of index 2. Thus we may choose the σ_i's such that $d = 2$ and the first condition in iv) of Theorem 4.3 holds. Assume additionally that exactly one σ_i is a 2-element (i.e., has order a power of 2) and the others have odd order. (Since G is generated by its elements of odd order, each element of G is a product of elements of odd order. It is easy from this to get such σ_i's, explicitly if so desired.) In the next paragraph we show that the second condition in iv) of Theorem 4.3 holds. Therefore i) follows.

Suppose that H is a nonsplit central extension of $G = \mathrm{PSL}_2(p)$ with $p > 3$. Then the commutator subgroup H' of H is perfect and it is a nonsplit central extension of G. From the above comments about the Schur multiplier group of G, $H' \cong \mathrm{SL}_2(p)$. We want to show that H cannot be generated by elements $\tau_1, \dots, \tau_r$ with $\tau_1 \cdots \tau_r = 1$, such that exactly one of them, say τ_1, is a 2-element $\neq 1$ and the others have odd order, and additionally, the order 2^m of τ_1 equals the order of the image of τ_1 in $\mathrm{PSL}_2(p)$. We may assume that the center of H is a 2-group. This forces $\tau_2, \dots, \tau_r$ to lie in H'. Hence also $\tau_1 = (\tau_2 \cdots \tau_r)^{-1} \in H'$ and so $H = H' \cong \mathrm{SL}_2(p)$. Raising τ_1 to the power 2^{m-1} would now yield a non-central involution in $\mathrm{SL}_2(p)$. But $\mathrm{SL}_2(p)$ has no non-central involution, which yields the desired contradiction.

The above example includes the case of the genus zero Galois cover of $\mathcal{P}^1_x$ with group $A_5 \cong \mathrm{SL}_2(5)$. Namely for the branch cycles $\sigma_1 = (1\,2)(3\,4), \sigma_2 = (1\,2\,3\,4\,5), \sigma_3 = (1\,5\,3)$. In this case it is trivially clear that G fixes a point of Pic^1 since this consists of just one point.

In general, the first statement in iv) will hold rarely since "d is too large."Consider that for every Sylow p-subgroup P of G, the minimal index in P of a cyclic subgroup divides d. This implies, for example, that the only simple groups for which iv) can hold are among the groups $\mathrm{PSL}_2(p)$ (p a prime), A_6 and A_7.

Remark 5.1: As in Part b) of the Remark after Corollary 2.5, we may develop a refined version for each prime p of the above equivalences. The same ideas show that for each prime p the following are equivalent:

5.1a) each (finite) unramified abelian p-extension of G splits:
b) the map $H^1(\mathcal{P}) \to H^1(\mathrm{Div}^0)$ is an isomorphism on the p-torsion subgroups:
c) the map from b) is surjective on the p-torsion subgroups; and
d) the p-torsion subgroup of the Schur multiplier of G is cyclic of order the p-part of d, and each (finite) unramified central p-extension of G splits.

In the special case $(d, p) = 1$ the equivalence of 5.1 b) and c) boils down to a well known result in group theory: *If G has a cyclic Sylow p-subgroup, then the Schur multiplier of G has no p-torsion* [CuR; Proposition 11.46].

§5.2. MAXIMAL SPLIT QUOTIENTS IN THE HURWITZ SEQUENCE: Consider again the Hurwitz sequence (*) from the introduction: $V_n \to {}_n\tilde{G} \to G$. In §4.2 we have characterized the Galois covers $\hat{X} \to \mathcal{P}^1_x$ with monodromy group G for which the Hurwitz sequence splits for each positive integer n. Here we consider the set of submodules W of V_n which are minimal with the following property:

5.2) the induced map ${}_n\tilde{G}/W \to G$ is a split extension of G.

Denote this set of submodules by $\mathcal{W}_{G,n}$. Its elements are in one-one correspondence with the set of equivalence classes of Galois covers $Y \to \mathcal{P}^1_x$ maximal with respect to factoring as $Y \to \hat{X} \to \mathcal{P}^1_x$, where $Y \to \hat{X}$ is unramified with abelian monodromy group V of exponent dividing n and the monodromy group of $Y \to \mathcal{P}^1_x$ splits over V (cf. Reminder 1.1).

Let *Phi* be the intersection of V_n with the frattini subgroup of ${}_n\tilde{G}$. Consider the quotients H of ${}_n\tilde{G}$ for which ${}_n\tilde{G} \to H$ is a frattini cover (§1.1) factoring through ${}_n\tilde{G} \to G$. The minimal such H is ${}_n\tilde{G}/\Phi$.

Proposition 5.2: *Each $W \in \mathcal{W}_{G,n}$ is contained in Φ (i.e., the natural map ${}_n\tilde{G} \to {}_n\tilde{G}/W$ is a frattini cover).*

Proof: Set $M = {}_n\tilde{G}/W$. To show that ${}_n\tilde{G} \to M$ is a frattini cover, we let S be a subgroup of ${}_n\tilde{G}$ that maps surjectively to M. We have to show this forces $S = {}_n\tilde{G}$. Since W is abelian, and ${}_n\tilde{G} = WS$, it is clear that $W \cap S$ is a normal subgroup of ${}_n\tilde{G}$. Denote the quotient ${}_n\tilde{G}/(W \cap S)$ by M'. Then $M' \to M$ has a splitting given by the image of S in M'. Clearly therefore $M' \to G$ splits, and thus the minimality of W implies that $W = W \cap S$, hence ${}_n\tilde{G} = WS = S$, as desired. □

The remainder of the paper gives a cohomological criterion for $\mathcal{W}_{G,n}$ to consist of more than one element. Then it will give an example where $G = A_8$, $n = 2$ and $\mathcal{W}_{G,n}$ has cardinality at least 2. First, however, we give a criterion for a given group extension of G with abelian kernel to be an unramified extension relative to suitable generators of G. Recall that a *p'-element* of G is an element of order relatively prime to p (for some prime p).

Lemma 5.3: *Let $H \to G$ be a surjective homomorphism of finite groups, with kernel V an elementary abelian p-group for some prime p. View V as a $Z/pZ[G]$ module. Assume this module has no non-zero quotient with trivial G-action. Then, if G is generated by its p' elements, the same is true for H. Further, there exist p' generators $\sigma_1, \dots, \sigma_r$ of G with $\sigma_1 \dots \sigma_r = 1$ and the map $H \to G$ is unramified relative to these generators.*

Proof: Let N be the subgroup of H generated by its p'-elements. Then, N is a normal subgroup of H. So, the commutator group $[N, V] = \langle g^{-1}v^{-1}gv : g \in N, v \in V \rangle$ lies in $N \cap V$. This implies N acts trivially in the quotient $V/(N \cap V)$.
If G is generated by its p'-elements, then N maps surjectively to G. Therefore, G acts trivially in $V/(N \cap V)$. By hypothesis, this implies $V/(N \cap V) = 0$. That is, $V \subset N$ and thus $H = N$. This proves H has p' generators.
Now we get the desired generators of G. Let $\tau_1, \dots, \tau_s$ be p' generators of H. Take $r = 2s$, $\sigma_{2i-1} = \tau_i'$, and $\sigma_{2i} = (\tau_i')^{-1}$, where τ_i' is the image of τ_i in G, $i = 1, \dots, s$. □
Note: For Frattini covers the conclusion that H has p' generators follows even if V has a Z/p quotient with trivial G action. The more serious question is this. Let $(\mathrm{C}_1, \dots, \mathrm{C}_r)$ be p' conjugacy classes of G. Denote their unique lifts to conjugacy classes of H of the same order also by $(\mathrm{C}_1, \dots, \mathrm{C}_r)$. Suppose $\boldsymbol{\sigma} \in \mathbf{C}$ generates G and satisfies $\sigma_1 \dots \sigma_r = 1$. When do such generators lift to H to give H unramified relative to these generators? Note also, the Hurwitz sequence ${}_p\tilde{G} \to G$ is universal for being able to lift any product-one generators $\boldsymbol{\sigma}$ of G. That is, $H \to G$ lifts $\boldsymbol{\sigma}$ if and only if it is a quotient of ${}_p\tilde{G} \to G$. So, the question is how to characterize this situation.

Proposition 5.4: *Let G be a finite group generated by its p'-elements, for some prime p. Let V be a $Z/p[G]$ module having submodules U_1 and U_2 with the following properties:*

5.3a) *the trivial module Z/pZ is not a quotient of V;*
b) *there exists $\alpha \neq 0$ in $H^2(G, V)$;*
c) *$U_1 \cap U_2 = 0$; and*
d) *under the natural map $H^2(G, V) \to H^2(G, V/U_i)$, α goes to 0, $i = 1, 2$..*

Then G has generators $\sigma_1, \dots, \sigma_r$ with $\sigma_1, \dots, \sigma_r = 1$ such that there are at least two elements in the set $\mathcal{W}_{G,p}$ of minimal submodules of V_p with split quotients (associated to the Hurwitz sequence relative to $\sigma_1, \dots, \sigma_r$).

Proof: Suppose $V \to H \to G$ is an extension corresponding to α as given in 5.3 b). Let $\sigma_1, \dots, \sigma_r$ be generators of G provided by Lemma 5.3. If $V_p \to {}_p\tilde{G} \xrightarrow{f} G$ is the associated Hurwitz sequence, then f factors as ${}_p\tilde{G} \xrightarrow{\nu} H \to G$. Set $U_i' = \nu^{-1}(U_i)$ for $i = 1, 2$. If $\mathcal{W}_{G,p}$ would consist of a unique element W, then $W \subset U_1' \cap U_2'$ by 5.3 d), hence the induced map ${}_p\tilde{G}/(U_1' \cap U_2') \to G$ is a split extension. But by 5.3 c), this extension is equivalent to the extension $H \to G$, which is non-split by 5.3.b). Hence the claim. □

Example 5.5: *$\mathcal{W}_{G,2}$ consists of at least two elements when $G = A_8$.* We are fortunate that Benson in [Bn] has given a convenient list from which we were able to find an example where the hypotheses of Proposition 5.4 are satisfied. In [Bn] there is a description of the Loewy layers of the projective indecomposable module corresponding to the irreducible module of A_8 of dimension 6. We will denote this irreducible module by **6**, and the trivial module by **1**. ([Bn] explains Loewy structure, but we refer the reader to [A; Chap. II] for the appropriate results from the theory of modular representations.)
It is helpful to display (just) the first 3 layers of the Loewy structures for the projective indecomposable modules for **1** and **6** (respectively):

5.4*a*)

						1								
			6		**14**		**20**$_1$			**20**$_2$				
1		**1**		**1**		**1**			**4**$_1$			**4**$_2$		**6**

5.4*b*)

							6							
				1		**4**$_1$		**4**$_2$		**14**				
				1		**6**		**6**		**6**				

The numbers indicate irreducible modules of the corresponding dimensions. Subscripts indicate that there are two such modules of the same dimension. Finally, while the Loewy structure captures some of the possibilities for submodules and quotient modules of the principal indecomposables, it does not do so unambiguously. For example, it is clear that there is a (unique) quotient module V of the principle indecomposable for **6** with a 2-layer Loewy structure consisting of a head with **6** and 2nd layer $\mathbf{4}_1 + \mathbf{4}_2$. On the other hand, it isn't clear from the principal indecomposable for **1** whether there exists a module with a 3-layer Loewy structure with the respective irreducibles **1**, **6** and $\mathbf{4}_i$.
We show that the module V of the last paragraph satisfies the hypotheses of Prop. 5.4. That is V has **6** at the top, and $U_i = \mathbf{4}_i$, $i = 1, 2$. Recall, as at the beginning of §2.2, that for any $Z/2Z[G]$ module M, $H^1(M) \neq 0$ is equivalent to the existence of a nonsplit extension N of M that fits in an exact sequence

$$0 \to M \to N \to \mathbf{1} \to 0.$$

We give the remainder of the example in two parts corresponding to the information we need about the exact cohomology sequence applied to the exact sequence

5.5) $$0 \to V \to V/U_1 \oplus V/U_2 \to \mathbf{6} \to 0.$$

Part 1: *$H^1(\mathbf{6}) \neq 0$ and $H^1(V/U_i) = 0$, $i = 1, 2$.* From Benson's diagram a quotient of the principal indecomposable for **1** has a module with two Loewy layers, **1** and **6**, respectively. This shows that $H^1(\mathbf{6}) \neq 0$. The module V/U_1, for example, has Loewy layers **6** and $\mathbf{4}_2$. There are two possibilities for the Loewy layers for a module L that is a non-split extension of **1** over V/U_1 : either there are three Loewy layers given by **1**, **6** and $\mathbf{4}_2$; or there are two Loewy layers with **1** and **6** on top and $\mathbf{4}_2$ in the second layer. Lemma 4.4.1 of [Be] shows that the former doesn't happen, while the latter would imply that L has a submodule L_1 whose two Loewy layers are **1** and $\mathbf{4}_2$ respectively. But then L_1 would be a quotient of the principal indecomposable for **1**. But a look at 5.4 a) shows that this doesn't happen.

Part 2: *Conclusion of the example.* Apply Part 1 to the exact sequence of cohomology obtained from 5.5):

$$0 \to H^1(\mathbf{6}) \to H^2(V) \to H^2(V/U_1) \oplus H^2(V/U_2)$$

is exact. Now choose any nonzero $\alpha \in H^1(\mathbf{6})$ regarded as an element of $H^2(V)$. Clearly α satisfies the hypotheses of Proposition 5.4. □

Bibliography

[A] J. L. Alperin, Local representation theory, *Cambridge studies in advanced mathematics* **11** (1986), Cambridge.

[Be] S. Beckmann, Galois coverings of fields of definition of solvable branched coverings, *Compositio Mathematica* **66** (1988), 121–144.

[Bn] D. Benson, The Loewy series for the projective indecomposable modules for A_8 and A_9, *Comm. in Alg.* **11** (1983), 1395–1451.

[B] D. Bloom, The subgroups of $\mathrm{SL}_3(q)$, *TAMS* **127** (1967), 150–178.

[CKK] J. Cossey, O. H. Kegel and L. G. Kovács, Maximal frattini extensions, *Archiv der Mathematik* **35** (1980), 210– 217.

[CuR] C. W. Curtis and I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Orders, Vol. 1, *Wiley, New York–Toronto* (1981).

[EFr] J. Ershov and M. Fried, Frattini covers and projective groups without the extension property, *Math. Annalen* **253** (1980), 233-239.

[Ga] W. Gaschütz, Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden, *Math. Z.* **60** (1954), 274–286.

[Gr] A. Grothendieck, Géometrie formelle et géometrie algébrique, *Seminaire Bourbaki* **t. 11, 182** (1958/59).

[GS] R. Griess and P. Schmid, The Frattini module, *Arch. Math.* **30** (1978), 256-266

[Gu] R. C. Gunning, Riemann surfaces and generalized theta functions, *Springer–Ergebnisse* **91** (1976).

[HS] P. Hilton and U. Stammbach, A Course in Homological Algebra, *Graduate Texts-Springer*, (1970), Berlin, Heidelberg, New York.

[Hu] B. Huppert, Endliche Gruppen, *Graduate Texts- Springer* (1967), Berlin, Heidelberg, New York.

[L,1] S. Lang, Abelian Varieties, *Interscience Tracts in Pure and Applied Mathematics 7* (1959), Interscience Publishers, New York.

[L,2] S. Lang, Introduction to Algebraic and Abelian Functions, *Springer Graduate Texts*, sec.ed. (1982), Berlin, Heidelberg, New York.

[Ma] H. Matzat, Konstruktive Galoistheorie, *Lecture notes in math, Springer–Verlag* **1284** (1986).

[N] D. G. Northcott, An introduction to homological algebra, *Cambridge Univ. Press* (1966).

[Se] J. P. Serre, Groupes algébrique et corps de classes, *Hermann, Paris* (1959).

Mike Fried and Helmut Völklein
Department of Mathematics
201 Walker Hall
University of Florida
Gainesville, Fl 32611

and

Mike Fried
Department of Mathematics
UC Irvine
Irvine, California 32611