Journal of Pure and Applied Algebra 43 (1986) 257–270
North-Holland

A GALOIS CORRESPONDENCE FOR RADICAL EXTENSIONS OF FIELDS

C. GREITHER
Math. Institut, Universität München, Theresienstrasse 39, D-8000 München 2, Fed. Rep. Germany

D.K. HARRISON
Dept. of Mathematics, University of Oregon, Eugene, OR 97403, USA

Communicated by M. Barr
Received 15 August 1985

In some sense the theory we develop is dual to the usual Galois theory of fields. We have chosen terminology to reflect that duality and to aid memory.

For K/k a finite extension of fields, we write

$$\mathrm{Cog}(K/k)=\{y\dot{k}\in\dot{K}/\dot{k}:\exists m>0 \text{ with } y^m\in\dot{k}\}.$$

Hence $\mathrm{Cog}(K/k)$ is the torsion subgroup of $\dot{K}/\dot{k}$. For H a subgroup of $\mathrm{Cog}(K/k)$, we write K_H for the set of all $a\in K$ such that a can be written $a=b_1+\cdots+b_n$ with $b_1\dot{k},\dots,b_n\dot{k}\in H$. We call K/k *cogalois* with cogalois group $\mathrm{Cog}(K/k)$ if:

(1) (*Conormality*) $\mathrm{card}(\mathrm{Cog}(K/k))$ is finite and at most $[K:k]$;

(2) (*Coseparability*) $K=K_H$ with $H=\mathrm{Cog}(K/k)$.

In the first section, we prove:

– If K/k is cogalois and E is a field between K and k, then K/E and E/k are cogalois.

– The maps $\mathrm{Cog}(-/k)$ and $K_{(-)}$ are inverse bijections between the lattices of intermediate fields of K/k, and of subgroups of $\mathrm{Cog}(K/k)$, respectively.

– There are many examples; e.g. $\mathbb{Q}(\sqrt[n_1]{a_1},\dots,\sqrt[n_t]{a_t})\subset\mathbb{R}$ $(a_i>0)$ is cogalois over $\mathbb{Q}$.

In the special case of simple radical extensions, our cogalois theory was essentially known (see Theorem 2.1 of Oroczo/Vélez [7]).

Let us remark that if K/k is cogalois, then it is a kH-galois object in the sense of [2] (also called an H-fully graded algebra). Our correspondence theorem is a sharpened version of the fundamental theorem of Galois theory in that setting (we get *all* subfields).

In the second section we study the connection between $G=\mathrm{Aut}(K/k)$ and $H=\mathrm{Cog}(K/k)$ in case K/k is both cogalois and galois. A somewhat surprising duality for a special class of nonabelian groups emerges, and we slightly enlarge the class of extensions where we can exhibit all intermediate fields.

In an appendix we prove that $\mathrm{Cog}(K/k)$ is always finite if K and k are algebraic number fields.

1.

Let K/k always be a finite extension of fields. Recall the definition of a cogalois extension from the introduction and observe that if K/k is cogalois, then $\mathrm{card}(\mathrm{Cog}(K/k))$ is exactly $[K:k]$. In other words, every set of representatives for $\mathrm{Cog}(K/k)$ forms a base of K over k. This will be used frequently.

At this moment, we give two examples: One can check directly that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is cogalois and $\mathrm{Cog}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})=\{\dot{\mathbb{Q}},\sqrt{2}\dot{\mathbb{Q}}\}$. $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is not cogalois since $\mathrm{Cog}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ contains three different elements $\dot{\mathbb{Q}},\sqrt{-3}\dot{\mathbb{Q}}$, $((-1+\sqrt{-3})/2)\dot{\mathbb{Q}}$.

Lemma 1.1. *If E is a field with $k\subset E\subset K$, then the following sequence is exact*

$$1\to \mathrm{Cog}(E/k)\to \mathrm{Cog}(K/k)\to \mathrm{Cog}(K/E).$$

Proof. This is quite easy to check. One can also take the exact sequence $1\to\dot{E}/\dot{k}\to\dot{K}/\dot{k}\to\dot{K}/\dot{E}$ and apply $(-)_{\mathrm{tor}}$.

Definition. K/k is *pure* if the following holds:
If $p=4$ or p prime, $\zeta\in K$, and $\zeta^p=1$, then $\zeta\in k$.

Examples. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is pure and $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is not.

Lemma 1.2. *If K/k is cogalois, then it is coseparable, separable and pure.*

Proof. (a) K/k is coseparable by definition.

(b) If K/k is not separable, we have $\mathrm{char}(k)=p$, k is infinite, and $p\mid[K:k]$. Since $[K:k]=\mathrm{card}(\mathrm{Cog}(K/k))$, there is an element $y\dot{k}\in\mathrm{Cog}(K/k)$ of precise order p; i.e., $y\notin k$ and $y^p\in\dot{k}$. Then for all $c\in k$, also $y+c\notin k$ but $(y+x)^p=y^p+c^p\in k$. It is quite easy to see that $(y+c)\dot{k}\neq(y+d)\dot{k}$ for $c\neq d\in k$. Therefore $\mathrm{Cog}(K/k)$ contains infinitely many elements $(y+c)\dot{k}$, $c\in k$. This is a contradiction.

(c) Now we show K/k is pure. Let $\zeta^p=1$, $\zeta\in K$. Assume first that p is prime. We may assume $\mathrm{char}(k)\neq p$ since $\mathrm{char}(k)=p$ implies $\zeta=1$. Since (if $\zeta\neq1$)

$$1+\zeta+\cdots+\zeta^{p+1}=0,$$

it is not the case that $1\dot{k},\dots,\zeta^{p-1}\dot{k}$ are distinct elements in $\mathrm{Cog}(K/k)$ (see the first observation of this section). Hence some $\zeta^i/\zeta^j\in k$ $(i\neq j)$, so $\zeta\in k$.

Next assume $p=4$, and again we may assume $\mathrm{char}(k)\neq2$, $\zeta\neq1$. One checks that $(1+\zeta)^4=-4\in\dot{k}$. But

$$1+\zeta-(1+\zeta)=0,$$

so it is not the case that the three elements $1\dot{k}, \zeta\dot{k}, (1+\zeta)\dot{k}$ of $\mathrm{Cog}(K/k)$ are distinct. But any of the three possible equality relations between them implies $\zeta \in k$.

The next lemma is the crucial step.

Lemma 1.3. *Assume $K=k(\alpha)$, $\alpha^p = a \in k$, $[K:k]=p$ prime, and K/k is pure and separable. Then K/k is cogalois.*

Proof. It is enough to show that the cyclic group with p elements $\langle \alpha\dot{k} \rangle$ makes up the whole of $\mathrm{Cog}(K/k)$.

Step 1. If q is a prime different from p, $\mathrm{Cog}(K/k)$ has no element of order q.

Proof. If $\mathrm{ord}(y\dot{k})=q$, we have $y^q = b \in k$. Since $[k(y):k]=q$ is impossible (q does not divide p), $x^q - b$ is reducible over k. By [3, p. 62], $x^q - b$ has a root β in k. Then $(y/\beta)^q = 1$, so by pureness $y/\beta \in k$, so $y \in k$. This contradicts $\mathrm{ord}(y\dot{k})=q$.

Step 2. $\mathrm{Cog}(K/k)$ has no element of order p^2.

Proof. Assume $\mathrm{ord}(yk)=p^2$, $y^{p^2} = b \in k$. Again $x^{p^2} - b$ must be reducible. If p is odd, b has a p-th root $\beta \in k$ by *loc.cit.* Then $(y^p/\beta)^p = 1$, so $y^p/\beta \in k$, so $y^p \in k$, which is a contradiction. If $p=2$ and b has a square root in k, the same argument works. If $p=2$ and b has no square root in k, then by loc.cit. $-4b = d^4$ for some $d \in k$. Hence $(d/y)^4 = -4$. Let $z = d/y$. Since

$$0 = z^4 + 4 = (z^2 - 2z + 2)(z^2 + 2z + 2),$$

either $z-1$ or $z+1$ is a fourth root of 1. Since K/k is pure, we get $z \in k$, so $y \in k$, which is again a contradiction.

Step 3. $\alpha\dot{k}$ generates $\mathrm{Cog}(K/k)$.

Proof. Take $y\dot{k} \in \mathrm{Cog}(K/k)$. By the first two steps, $y^p \in k$ and we may assume $y \notin k$. Thus $k(y) = K$.

Let $E = k(\zeta)$ be a splitting field of $x^p - 1$ over k, with ζ a primitive p-th root of 1. Note $\mathrm{char}(k) \neq p$ because K/k is separable. Let

$$L = K(\zeta) = E(\alpha).$$

We have $[L:K] \leq p-1$, $[E:k] \leq p-1$. (Actually, both $[L:K]$ and $[E:k]$ divide $p-1$). Moreover

$$p \cdot [L:K] = [L:k] = [L:E][E:k],$$

so $p \mid [L:E] = p$ and $\alpha \notin E$. Therefore $L \mid E$ is a p-Kummer extension. Let

$$A = \{\beta \in \dot{L} \mid \beta^p \in \dot{E}\}.$$

Note y and α are in A. By [1, Theorem 24], $A/\dot{E}$ is cyclic of order p. Since $\alpha \notin \dot{E}$, this implies

$$y = \alpha^i e \quad \text{for some } i \in \mathbb{N},\ e \in \dot{E}.$$

Hence we have, with $y^p = d \in k$,

$$d = a^i e^p.$$

Let $\Gamma = \mathrm{Aut}(E/k)$. The exact sequence

$$1 \to \langle \zeta \rangle \to \dot{E} \xrightarrow{(-)^p} \dot{E}^p \to 1$$

gives an exact sequence

$$\dot{E}^\Gamma \xrightarrow{(-)^p} (\dot{E}^p)^\Gamma \to H^1(\Gamma, \langle \zeta \rangle)$$

with the last group trivial because ord(Γ) and $\mathrm{ord}\langle \zeta \rangle = p$ are coprime. Since $e^p = d/a^i$ is in $(\dot{E}^p)^\Gamma$, we get

$$e^p = g^p \quad \text{for some } g \in \dot{E}^\Gamma = \dot{k}.$$

Thus $d = a^i g^p = y^p$. Hence $y/(\alpha^i g)$ is a p-th root of 1 and has to be in k. Thus $y \in \alpha^i \dot{k}$.

Remark. There is a short proof of 1.3 which uses Theorem 1.7 of [6]. The proof of that theorem needs a condition on the characteristic, which is not explicit in the statement of the theorem.

Lemma 1.4. *If E is a field between k and K, and E/k and K/E are both conormal, then K/k is conormal.*

Proof. By definition, E/k is conormal if and only if $\mathrm{card}(\mathrm{Cog}(E/k)) \leq [E:k]$. The lemma is a direct consequence of Lemma 1.1.

The reason why we defined pureness is the following result:

Theorem 1.5. *K/k is cogalois if and only if K/k is coseparable, separable and pure.*

Proof. The 'only if' part was proved in Lemma 1.2. Let us prove the 'if' part. We choose a finite subgroup G of $\mathrm{Cog}(K/k)$ such that $K_G = K$. This is possible since $K_{\mathrm{Cog}(K/k)} = K$ by hypothesis and K/k is finite. There is a chain

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_m = G$$

of subgroups of G such that H_i/H_{i-1} is cyclic of order p_i, where p_i is a prime number for all $i = 1, \ldots, m$. Thus $K_{H_i}/K_{H_{i-1}}$ is pure (because K/k is pure), and it is coseparable by construction. Since H_i/H_{i-1} is cyclic of order p_i, K_{H_i} is obtained from $K_{H_{i-1}}$ by adjoining a p_i-root. Since K/k is separable, so is $K_{H_i}/K_{H_{i-1}}$. By 1.3, $K_{H_i}/K_{H_{i-1}}$ is cogalois, and thus conormal. By an inductive application of 1.4, K/k is conormal. Thus K/k is cogalois.

This result enables us to prove the main theorem. The statement is this:

Theorem 1.6. *Assume K/k is a cogalois extension.*
(a) *For every intermediate field $k \subset E \subset K$, K/E and E/k are again cogalois.*
(b) *For every intermediate field $k \subset E \subset K$, we have $K_{\mathrm{Cog}(K/k)} = E$.*
(c) *For every subgroup $U \leq \mathrm{Cog}(K/k)$, we have $\mathrm{Cog}(K_U/k) = U$.*
(d) *The maps $\mathrm{Cog}(-/k)$ and $K_{(-)}$ are inverse isomorphisms of lattices.*
(e) *$\mathrm{Cog}(K/E)$ is canonically isomorphic to $\mathrm{Cog}(K/k)/\mathrm{Cog}(E/k)$.*

Proof. (a) By 1.5, K/k is coseparable, separable and pure. From this it follows that K/E is coseparable, separable and pure. Applying 1.5 again, we get that K/E is cogalois. In particular K/E is conormal. By counting group orders and using Lemma 1.1, one sees that $\mathrm{Cog}(K/k)$ cannot have fewer than $[E:k]$ elements. If $e_1\dot{k}, \dots, e_r\dot{k}$ is a listing of $\mathrm{Cog}(K/k)$, then the $e_i\dot{k}$ are also distinct elements of $\mathrm{Cog}(K/k)$, so $e_i, \dots, e_r$ are k-linearly independent. Therefore the e_i are a base of E/k, and E/k is cogalois.

(b) Clearly $K_{\mathrm{Cog}(E/k)} \subset E$. But one sees that $[K_{\mathrm{Cog}(E/k)} : k] = \mathrm{card}(\mathrm{Cog}(E/k))$, and $[E:k] = \mathrm{card}(\mathrm{Cog}(E/k))$ by (a). Hence we have equality.

(c) Cleary $H \subset \mathrm{Cog}(K_H/k)$. By (a), $\mathrm{card}(\mathrm{Cog}(K_H/k)) = [K_H : k]$, and obviously $[K_H : k] \leq \mathrm{card}(H)$, so we have equality.

(d) Follows from (b) and (c).

(e) One has a natural injection $\mathrm{Cog}(K/k)/\mathrm{Cog}(E/k) \to \mathrm{Cog}(K/E)$ by Lemma 1.1. It has to be surjective because the orders of the groups are equal.

We close this section with some more examples.

(a) Let $a_1, \dots, a_t$ be positive rational numbers, $n_i \in \mathbb{N}$, and $K = \mathbb{Q}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_t]{a_t}) \subset \mathbb{R}$. Then it is trivial that $K/\mathbb{Q}$ is pure since $K \subset \mathbb{R}$. $K/\mathbb{Q}$ is obviously coseparable, so by 1.5 it is cogalois. This means that all intermediate fields E are generated by monomials in the roots $\sqrt[n_i]{a_i}$.

Remark. One can always determine the intermediate fields of a coseparable extension K/k by adjoining enough roots of unity to K (this gives the field K', say) and then determining all groups between $G_0 = \mathrm{Aut}(K'/K)$ and $G' = \mathrm{Aut}(K'/k)$. This can be trickier than one might expect. We offer $\mathbb{Q}(\sqrt[10]{5})/\mathbb{Q}$ as an example. Note that $\mathbb{Q}(\sqrt[10]{5})$ and $\mathbb{Q}(\zeta_{10})$ are not linearly disjoint. By cogalois theory we get at once that there are only four subfields: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt[5]{5})$, and $\mathbb{Q}(\sqrt[10]{5})$.

(b) Let p be any odd prime. Take $k = \mathbb{Q}(\zeta_p)$ and take $K = \mathbb{Q}(\zeta_{p^n})$ ($n \in \mathbb{N}$ arbitrary). Again, K/k is certainly coseparable and separable. K/k is even cogalois: To show purity, one can use that $\mathbb{Q}(\zeta_{p^n})$ and $\mathbb{Q}(\zeta_q)$ are linearly disjoint whenever $q \neq p$ is a prime or $q = 4$.

Remark. Of course, for this extension the intermediate fields are well-known since it is an abelian galois extension. The interesting cogalois extensions are a mixture of type (a) and (b) (see the next section), and they usually are not abelian even if they are galois.

2.

We assume throughout this section that $\mathrm{char}(k)=0$. F/k is always a finite field extension. We intend to examine extensions which are cogalois and galois at the same time, to exhibit a duality between the involved cogalois and galois groups, and to generalize a little.

Definition. F/k is called a *cn-extension* ('coseparable and normal') if F is the splitting field of some polynomial $(X^{n_1}-a_1)\cdot\ldots\cdot(X^{n_t}-a_t)$ with $n_i\in\mathbb{N}$ and $a_i\in k$.

Notation. $F=k\langle n_1,a_1;\ldots;n_t,a_t\rangle$ is a *neat presentation* if a_i, n_i are such that for p dividing any n_i, k already contains a primitive p-th root of unity. Here p runs over the set of primes united with $\{4\}$.

Remarks 2.1. (a) F is cn over k if and only if F/k is coseparable and normal. This justifies the name 'cn-extension'.

(b) If F/k is cn and cogalois, then it has a neat presentation.

Proof. (a) The 'only if' part is clear.

Suppose F/k is coseparable and normal. Write $F=K_H$ with $H\leq\mathrm{Cog}(F/k)$ finite, and write $H=\langle y_1\dot{k}\rangle\oplus\cdots\oplus\langle y_t\dot{k}\rangle$ with $\mathrm{ord}(y_i\dot{k})=q_i=p_i^{e_i}$ a prime power. We claim $F=k\langle n_1,a_1;\ldots;n_t,a_t\rangle$ with $a_i=y_i^{q_i}$. For this we need that $X^{q_i}-a_i$ splits completely in F; i.e., F contains a primitive q_i-th root of unity. Since F is normal, F contains all conjugates $y_i\zeta_1,\ldots,y_i\zeta_r$ of y_i over k. Here all ζ_j are q_i-th roots of 1. Just suppose no ζ_j is primitive. Since every conjugate of $y_i^{(q_i/p_i)}$ is a (q_i/p_i)-th power of a conjugate of y_i, this implies that $y_i^{(q_i/p_i)}$ is equal to all its conjugates, so $y_i^{(q_i/p_i)}\in k$, which is a contradiction.

(b) Let p be prime or $p=4$, and $p\,|\,n_i$. We must show $\zeta_p\in k$. But obviously $\zeta_p\in F$ because $X^{n_i}-a_i$ splits completely over F. Since F/k is pure (see 1.3), ζ_p is in k.

Now let F/k be a cn-extension. Note F/k is galois. Let $G=\mathrm{Aut}(F/k)$ and $H=\mathrm{Cog}(F(k))$. There is a canonical map

$$\sigma: G\times H\to\mu(F)=\{\zeta\in F\,|\,\zeta\text{ root of unity}\}$$
$$(g,y\dot{k})\to g(y)\cdot y^{-1}.$$

G operates on $\mu(F)$, $\sigma(g,-)$ is linear on H, and $\sigma(-,y\dot{k})$ is an element of

$$X(G)=\{\chi: G\to\mu(F)\,|\,\chi\text{ crossed homomorphism}\}.$$

(Recall χ is a crossed homomorphism if $\chi(gg')=\chi(g)\cdot {}^g\chi(g')$.) σ is non-degenerate in the following sense: If $\sigma(g,H)=1$, then $g=\mathrm{id}$. If $\sigma(G,y\dot{k})=1$, then $y\in\dot{k}$. Therefore σ induces a monomorphism

$$H\to X(G).$$

For $U\leq G$ a subgroup, define

$$H\geq U^{\perp}=\{h\in H\,|\,\sigma(U,h)=1\}.$$

We would like σ to be a perfect pairing; i.e., $\perp$ is a duality (anti-isomorphism) of lattices: $\mathrm{Subgroups}(G)\to\mathrm{Subgroups}(H)$.

Theorem 2.2. *If F/k cogalois, then for $U\leq G$ we have* $\mathrm{Fix}(U)=K_{(U^{\perp})}$, *and $\perp$ is a duality from* $\mathrm{Subgroups}(G)$ *onto* $\mathrm{Subgroups}(H)$.
(For $W\leq H, K_W$ is defined as in the introduction.)

Proof. $K_{(U^{\perp})}$ is fixed under U by definition. Just suppose $\mathrm{Fix}(U)\lneqq K_{(U^{\perp})}$. By cogalois theory, $\mathrm{Fix}(U)=K_{W}$, $W\lneqq U^{\perp}$. Pick $w\dot{k}\in W\setminus U^{\perp}$. Then $w\in\mathrm{Fix}(U)$, so $w\dot{k}\in U^{\perp}$; hence we have a contradiction.

Since the map $\mathrm{Fix}(-)$ is a duality, and $K_{(-)}$ is an isomorphism of lattices, $(-)^{\perp}$ must be a duality of lattices.

Example (of a non-abelian galois and cogalois extension). Take $k=\mathbb{Q}(\zeta_3)$, $F=k(\sqrt[9]{5},\zeta_9)$. Then $[F:k]=27$ and F/k is coseparable. One checks that $\zeta_4\notin F$ and $\zeta_p\notin F$ for all odd primes $p\neq 3$ (use that $k(\sqrt[9]{5})(\zeta_4)$ is quadratic over $k(\sqrt[9]{5})$ but F is cubic over $k(\sqrt[9]{5})$,and use that $p-1$ does not divide $54=[F:\mathbb{Q}]$ for any odd prime $p\neq 3$). Thus F/k is cogalois, and $C=\mathrm{Cog}(F/k)$ is generated by $x\dot{k}$ and $y\dot{k}$ of order 9 and 3 respectively, with $x=\sqrt[9]{5}$, $y=\zeta_9$. Now $G=\mathrm{Aut}(F/k)$ is generated by α and β of order 9 and 3 respectively, where $\alpha(x)=yx$, $\alpha(y)$ and $\beta(x)=x$, $\beta(y)=y^4$. The pairing σ is given by $\sigma(\alpha,x\dot{k})=\zeta_9$, $\sigma(\beta,x\dot{k})=1$ and $\sigma(\alpha,y\dot{k})=1$, $\sigma(\beta,y\dot{k})=\zeta_9^3=\zeta_3$. We illustrate the resulting duality between subgroups of G and subgroups of C by just one nontrivial example: Let $D\subset C$ be the group of order 3 generated by $x^3y\dot{k}$. Then $D^{\perp}\subset C$ has order 9 and is generated by $\alpha\beta^{-1}$. (Check that $\sigma(\alpha\beta^{-1},x^3y\dot{k})=1$, and check that $(\alpha\beta^{-1})^9=\mathrm{id}$.) In a similar way, the reader may list the complete duality. G is a non-abelian group, for instance $\beta\cdot\alpha\cdot\beta^{-1}=\alpha^4$.

In order to understand the group-theoretical pattern behind this duality, we generalize 2.2 to the case of extensions with neat presentations. First we exhibit a class of groups G such that there is a duality between $\mathrm{Subgroups}(G)$ and $\mathrm{Subgroups}(X(G))$. (For the definition of $X(G)$, the group of 'crossed characters', see below.) The final result is:

Theorem 2.3. *Assume $F=k\langle n_1,a_1;\dots;n_t,a_t\rangle$ is a neat presentation. Then any intermediate field $E, F\supset E\supset k$, is generated by monomials in roots of $X^{n_i}-a_i$.*

We begin with the group-theoretical results. For any $r \in \mathbb{N}$, we say that $m \in \mathbb{N}$ is *related* to r, if m divides r, every prime p dividing r also divides m, and $4 \mid m$ in case $4 \mid r$. Let $D_{r,m}$ (or D, if r and m are fixed) be the kernel of the natural epimorphism

$$(\mathbb{Z}/(r))^{\cdot} \to (\mathbb{Z}/(m))^{\cdot}.$$

We suppose here that r is related to m.

Let $1 \to H \to G \to D_{r,m} \to 1$ be an extension of groups. We say it is *allowable* if H is finite abelian of exponent dividing r, and if the induced operation of $D_{r,m}$ on H is the natural one, i.e., the action by scalar multiplication. *Example*: $G = H \ltimes D_{r,m}$, the split allowable extension.

For the next lemma and theorem, we assume that G is an allowable extension of $D_{r,m}$ by H. G operates through $D_{r,m}$ on the additive group $\mathbb{Z}/(r)$ (by scalar multiplication), so the following makes sense for all subgroups $U \leq G$:

$$X(U) = \{\chi : U \to \mathbb{Z}/(r) \mid \chi \text{ crossed homomorphism}\}.$$

Lemma 2.4. (a) $\mathrm{card}(X(G)) \geq \mathrm{card}(G)$.

(b) *For* $U \leq V \leq G$ *we have* $\mathrm{card}(\mathrm{Ker}(X(V) \to X(U)) \leq [V : U]$. *In particular,* $\mathrm{card}(X(V))/\mathrm{card}(X(U)) \leq [V : U]$.

(c) *For* $U \leq V \leq G$ *the restriction map* $X(V) \to X(U)$ *is surjective, and* $\mathrm{card}(X(U)) = \mathrm{card}(U)$ *for all* $U \leq G$.

(d) *For* $U \lneq V \leq G$, *there is a* $\chi \in X(V)$ *with* $\chi(U) = 0$, $\chi(V) \neq 0$.

Proof. (a) Let $B(G) \subset X(G)$ be the subgroup of inner crossed homomorphisms $\chi_a, a \in \mathbb{Z}/(r)$. ($\chi_a(g) = {}^g a - a$.) There is a canonical exact sequence

$$0 \to (\mathbb{Z}/(r))^G \to \mathbb{Z}/(r) \to B(G) \to 0.$$

Moreover, it is not hard to check that $(\mathbb{Z}/(r))^G = (\mathbb{Z}/(r))^{D_{r,m}} = (r/m)\mathbb{Z}/(r)$. Thus $\mathrm{card}(B(G)) = r/m$.

By definition of $H^1(G, \mathbb{Z}/(r)) = X(G)/B(G)$, we have

$$\begin{aligned} \mathrm{card}(X(G)) &= \mathrm{card}(H^1(G, \mathbb{Z}/(r))) \cdot \mathrm{card}(B(G)) \\ &= \mathrm{card}(H^1(G, \mathbb{Z}/(r))) \cdot r/m. \end{aligned}$$

Since $\mathrm{card}(G) = \mathrm{card}(H) \cdot \mathrm{card}(D_{r,m}) = \mathrm{card}(H) \cdot (r/m)$, we only have to show

$$\mathrm{card}(H^1(G, \mathbb{Z}/(r))) \geq \mathrm{card}(H).$$

The following exact sequence comes from the Lyndon–Hochschild spectral sequence (see [4, p. 354]):

$$H^1(G, \mathbb{Z}/(r)) \xrightarrow{\text{res}} H^1(H, \mathbb{Z}/(r))^G \to H^2(D_{r,m}, (\mathbb{Z}/(r))^H).$$

We observe:

(i) H operates trivially on $\mathbb{Z}/(r)$, and $rH = 0$, so $H^1(H, \mathbb{Z}/(r)) = \mathrm{Hom}(H, \mathbb{Z}/(r))$ has exactly $\mathrm{card}(H)$ elements.

(ii) The operation of G on $H^1(H, \mathbb{Z}/(r))$ comes from conjugation. G operates on H and $\mathbb{Z}/(r)$. On both groups, G operates through $D_{r,m}$ by scalar multiplication. Since $H^1(H, \mathbb{Z}/(r)) = \mathrm{Hom}_{\mathbb{Z}}(H, \mathbb{Z}/(r))$, the operation of G on $H^1(H, \mathbb{Z}/(r))$ is trivial.

(iii) Note that H operates trivially on $D_{r,m}$. By (i) and (ii) it suffices now to show that res is surjective, and we even show that $H^2(D_{r,m}, \mathbb{Z}/(r)) = 0$. From elementary number theory one knows that $D_{r,m}$ is cyclic, so

$$H^2(D_{r,m}, \mathbb{Z}/(r)) \cong H^0(D_{r,m}, \mathbb{Z}/(r)).$$

We claim the latter group is zero, i.e., $[\mathbb{Z}/(r)]^{D_{r,m}} = N_{D_{r,m}}(\mathbb{Z}/(r))$. Let $D = D_{r,m}$. We already know that $[\mathbb{Z}/(r)]^D = (r/m)\mathbb{Z}/(r)$, so it suffices to show that $r/m + (r)$ is a norm from $\mathbb{Z}/(r)$ under D. Consider

$$N_D(1) \equiv \sum_{(y \bmod r/m)} (1 + ym)$$

$$\equiv \frac{r}{m} + \frac{1}{2}\frac{r}{m}\left(\frac{r}{m} - 1\right) m \equiv \frac{r}{m} + \frac{ra}{2} \pmod r$$

with $a = (r/m) - 1 \in \mathbb{Z}$.

Claim. r/m is an integral multiple of $r/m + (ra)/2 \bmod r$.

Case 1: *r/m is odd.* Then a is even and $r/m + (ra)/2 \equiv r/m \bmod r$, and there is nothing to prove. *Case* 2: *r/m is even.* Since m is related to r, 8 must divide r, and $4 \mid m$. We then have

$$\left(\frac{r}{m} + \frac{ra}{2}\right)\left(1 - \frac{ma}{2}\right) \equiv \frac{r}{m} + \frac{ra}{2} - \frac{ra}{2} - \frac{ram^2}{4}$$

$$\equiv \frac{r}{m} - \frac{m}{4} ra^2 \equiv \frac{r}{m} \pmod r,$$

so r/m is an integral multiple of $r/m + (ra)/2 \bmod r$, as claimed.

(b) By induction, one can perform a reduction to the case that there are no groups properly between U and V.

It is easy to check the following:

(i) There is an element $y \in V \setminus U$ with $y^p \in U$.

(ii) U and y generate V.

(iii) $[V:U]$ is at least p. (Consider the cosets $y^j \cdot U$, $j = 0, \dots, p-1$.)

Now let $\chi \in \mathrm{Ker}(X(V) \to X(U))$. We have to show that there are at most p choices for χ. By (ii), it suffices to show that we have at most p possible values for $\chi(y)$.

Let $1 + ma \pmod r$ be the image of y in $D_{r,m}$. By repeated use of the definition of a crossed homomorphism we get:

$$0 = \chi(y^p) = \chi(y) + (1 + ma)\cdot\chi(y) + \cdots + (1 + ma)^{p-1}\cdot\chi(y)$$

$$= c \cdot \chi(y) \quad \text{with } c = \sum_{i=0}^{p-1} (1 + ma)^i.$$

Claim. c and $p \pmod r$ are associated in the ring $\mathbb{Z}/(r)$.

If the claim is established, it follows at once that the equation $0 = c \cdot \chi(y)$ has at most p solutions in $\mathbb{Z}/(r)$, and we are done.

Proof of the Claim. We have to establish two facts:

(α) If a prime $q \neq p$ divides r, then q does not divide c.

(β) If $p \mid r$, then $p \mid c$. If $p^2 \mid r$, then p^2 does not divide c.

Proof of (α). We also have $q \mid m$. Then $c \equiv \sum_{i=0}^{p-1}(1+0) \equiv p \pmod q$.

Proof of (β). We have $c \equiv \sum_{i=0}^{p-1}(1+0) \equiv 0 \pmod p$. Assume now $p^2 \mid r$. Since $p^2 \mid m^2$, the binomial theorem yields the following congruence $\operatorname{mod} p^2$:

$$c \equiv \sum_{i=0}^{p-1} (1 + ima) \equiv p + m\,a\,p\,\frac{p-1}{2} \pmod{p^2}.$$

If $p \neq 2$, then p^2 divides $m\,a\,p(p-1)/2$, so $c \equiv p \pmod{p^2}$. If $p = 2$, then (since $4 \mid r$) 4 already divides m, and we again get $c \equiv 2 \pmod 4$.

(c) Consider $\{e\} \leq U$. By (b), $\operatorname{card}(X(U)) \leq [U : e] = \operatorname{card}(U)$. Again by (b), $\operatorname{card}(\operatorname{Ker}(X(G) \to X(U))) \leq [G : U]$. Finally, (a) says that $\operatorname{card}(X(G)) \geq \operatorname{card}(G) = \operatorname{card}(U) \cdot [G : U]$. Taking these together, we get that all three inequalities are equalities and $X(G) \to X(U)$ is surjective. This implies that also $X(V) \to X(G)$ is surjective.

(d) Since $\operatorname{card}(X(V)) > \operatorname{card}(X(U))$ by (c), the restriction map $X(V) \to X(U)$ cannot be injective. Take any $\chi \neq 0$ in $\operatorname{Ker}(X(V) \to X(U))$.

Now we define a duality between subgroups of G and subgroups of $X(G)$. Let $\langle -, - \rangle$ denote the evaluation map $G \times X(G) \to \mathbb{Z}/(r)$. For $U \leq G$ and $W \leq X(G)$ let

$$U^{\perp} = \{\chi \in X(G) \mid \langle U, \chi \rangle = 0\},$$
$$W^{\perp} = \{g \in G \mid \langle g, W \rangle = 0\}.$$

One verifies that $U^{\perp}$ and $W^{\perp}$ are again subgroups.

Theorem 2.5. *The assignments* $(-)^{\perp}$ *define mutually inverse order-inverting bijections between the lattices* Subgroups(G) *and* Subgroups($X(G)$).

Proof. Obviously we have $U^{\perp\perp} \supset U$ and $W^{\perp\perp} \supset W$ in the above notation. But 2.4(d) implies that $U^{\perp\perp} = U$.

On the other hand, every $g \in G$ defines an element g' in $\operatorname{Hom}(X(G), \mathbb{Z}/(r))$, and $g' = 0$ implies $g = e$ by 2.4(d). Since $X(G)$ is abelian of exponent dividing r, and

$$\operatorname{card}(\operatorname{Hom}(X(G), \mathbb{Z}/(r)) = \operatorname{card}(X(G)) = \operatorname{card}(G),$$

the map $g \to g'$ is a bijection from G onto $\operatorname{Hom}(X(G), \mathbb{Z}/(r))$. From the duality theory of finite abelian groups it follows that for any $W \lneq W' \leq X(G)$ there exists $F \in \operatorname{Hom}(X(G), \mathbb{Z}/(r))$ with $F(W) = 0$, $F(W') \neq 0$. Now $F = g'$ for some $g \in G$, so $\langle g, w \rangle = 0$, $\langle g, W' \rangle \neq 0$. This yields $W^{\perp\perp} = W$, which proves the theorem.

Now we return to the field-theoretic situation.

Proof of 2.3. Let r be the least common multiple of all n_i. Then F contains a primitive r-th root ζ of unity. Let $H = \mathrm{Aut}(F/k(\zeta))$, $G = \mathrm{Aut}(F/k)$, $D = \mathrm{Aut}(k(\zeta)/k)$. Then we have an exact sequence

$$(*) \qquad 1 \to H \to G \to D \to 1.$$

D is canonically a subgroup of $(\mathbb{Z}/(r))^{\cdot}$. (Identify τ with $\bar{x}$ if $\tau(\zeta) = \zeta^x$.) We claim that D is of the form $D_{r,m}$. For this, define m' to be the product of all primes dividing r if $4 \nmid r$ and twice the latter product if $4 \mid r$. m' is the smallest divisor of r related to r. $D_{r,m'}$ is cyclic, and the hypotheses in 2.3 concerning roots of unity ensure that $D \subset D_{r,m'}$. The order of D divides $\mathrm{card}(D_{r,m'}) = \phi(r)/\phi(m') = r/m'$, so it has the form r/m with $m' \mid m \mid r$. Since $D_{r,m'}$ is cyclic, it contains exactly one subgroup with r/m elements, and therefore $D = D_{r,m}$. One can check now that $(*)$ is allowable; i.e., D operates on H by scalar multiplication.

Pick $\alpha_i \in F$ with $\alpha_i^{n_i} = a_i$. Let $C \leq \mathrm{Cog}(F/k)$ be the subgroup generated by $\zeta\dot{k}$ and all $\alpha_i\dot{k}$. We shall prove that C is canonically isomorphic to $X(G)$. Note $F = K_C$; i.e., F is generated by C. We consider the canonical pairing as in 2.2

$$\sigma : G \times C \to \mu_r(F) \cong \mathbb{Z}/(r)$$
$$(g, c\dot{k}) \mapsto g(c) \cdot c^{-1},$$
$$\zeta \mapsto \bar{1}.$$

σ is linear on C and crossed-linear on G. (G operates canonically on $\mu_r(F) \subset F$.) Moreover, if $\sigma(G, y\dot{k}) = 1$, then $y \in \dot{k}$, so σ gives rise to an embedding of C into

$$X(G) = \{\chi : G \to \mathbb{Z}/(r) \mid \chi \text{ crossed homomorphism}\}.$$

From 2.5 we now get that $\mathrm{card}(X(G)) = \mathrm{card}(G) = [F:k]$. Since $F = K_C$, we must have $\mathrm{card}(C) \geq [F:k]$. Thus C is naturally isomorphic to $X(C)$, and $\mathrm{card}(C) = [F:k]$, so C forms a k-base of F.

Now take any subfield E of F/k and let $s = [F:E]$. Then $E = \mathrm{Fix}(U)$ where U is a subgroup of order s in G.

By 2.4(c), $U^{\perp} = \mathrm{Ker}(X(G) \to X(U))$ has index s in C. The field $K_{(U^{\perp})}$ is contained in $\mathrm{Fix}(U) = E$. Since C forms a k-base of F, $[K_{(U^{\perp})} : k] = \mathrm{card}(U)$, so $[F : K_{(U^{\perp})}] = [H : U^{\perp}] = s = [F:E]$, so $E = K_{(U^{\perp})}$. This means that E is generated by certain monomials in ζ and the α_i.

Remark. This proof actually yields a lattice isomorphism from k-Subfields(F) onto Subgroups(C), in analogy to 1.6. Note that C is in general not the whole of $\mathrm{Cog}(F/k)$.

Since $X(G)$ is abelian, Theorem 2.5 implies that Subgroups(G) has an inclusion-inverting involution θ with $|\theta(U)| = |G|/|U|$ for all $U \leq G$.

Theorem 2.6. *Let G be a finite group such that there exists an inclusion-inverting involution θ of* Subgroups(G) *with $|\theta(U)| = |G|/|U|$ for all $U \leq G$. Then G is an allowable extension.*

Proof. G is called *quasi-hamiltonian* if $UV = U * V$ for all $U, V \leq G$. ($U * V = \langle U \cup V \rangle$.) First we show this is the case for G. We must show $|U * V| \leq |U|\,|V|/|U \cap V|$. This formula is equivalent to each of the following:

$$|G|/|U*V| \geq |G| \cdot |G| \cdot |U \cap V|/(|U| \cdot |V| \cdot |G|),$$

$$|\theta(U) \cap \theta(V)| \geq |\theta(U)| \cdot |\theta(V)|/|\theta(U \cap V)|,$$

$$|\theta(U) \cap \theta(V)| \geq |\theta(U)| \cdot |\theta(V)|/|\theta(U) * \theta(V)|.$$

The last inequality is equivalent to

$$|\theta(U) * \theta(V)| \geq |\theta(U)| \cdot |\theta(V)|/|\theta(U) \cap \theta(V)|,$$

and this is indeed true.

By [5, Theorem 7], G is nilpotent and all p-Sylow subgroups G_p of G have modular lattices of subgroups. For odd p, one knows that G_p cannot be hamiltonian if it is non-abelian. For $p = 2$, this is also true. (Suppose G_2 non-abelian hamiltonian. Then the quaternion group Q is a factor of G_2, and of G. Using θ, one finds an 8-element subgroup $U \leq G$ with Subgroups(U) anti-isomorphic to Subgroups(Q). One checks that no such U exists.)

By [5, Theorem 14], G_p is abelian or the following holds: There is $N \lhd G$, $s \in \mathbb{N}$ ($s \geq 2$ if $p = 2$) and $t \in G$ such that $G/N = \langle \bar{t} \rangle$ is cyclic, N is abelian, and t acts on N as multiplication by $1 + p^s$. Let $p^e = \operatorname{ord}(\bar{t})$. One checks that $1 + p^s$ has order p^e in $(\mathbb{Z}/(p^{e+s}))^{\cdot}$. Hence we get a commutative diagram ($f(\bar{t}) = 1 + p^s$):

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, equal] & G \arrow[r] \arrow[d, equal] & G/N \arrow[r] \arrow[d, "f", "\cong"'] & 1 \\
1 \arrow[r] & N \arrow[r] & G \arrow[r] & D_{p^{s+e}, p^s} \arrow[r] & 1
\end{tikzcd}$$

and in the lower extension, D_{p^{s+e}, p^s} operates on N by scalar multiplication. Thus G is an allowable extension if we can show that $\exp(N)$ divides p^{s+e}.

Just suppose it did not. Then multiplication by $1 + p^{s+e}$ is not the identity on N. By definition of e, multiplication by $(1 + p^s)^{p^e}$ is the identity on N. But since for $n \gg 0$, $1 + p^{s+e}$ and $(1 + p^s)^{p^e}$ generate the same subgroup of $(\mathbb{Z}/(p^n))^{\cdot}$ (use that $D_{p^n, p}$ is cyclic for p odd, and $D_{2^n, 4}$ cyclic), this is a contradiction.

We showed that all G_p are allowable extensions. (If G_p is abelian, this holds anyway.) So we have

$$1 \to N_p \to G_p \to D_{r(p), m(p)} \to 1.$$

It is not hard to see that (setting $r=\prod r(p)$, $m=\prod m(p)$, $N=\prod N_p$) G is an allowable extension of $D_{r,m}$ by N.

Remark 2.7. The class of extensions covered by 2.3 does not seem much larger than the class of cogalois extensions considered in 2.2. (One example distinguishing these two classes is $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$, which is covered by 2.3 but not by 2.2.) Nevertheless, 2.3 has the following advantage: In general it is much easier to establish that F/k has a neat presentation than to prove that F/k is pure (which involves hunting for roots of unity in F and deciding whether they are already in k). Another point is that the class of fields with neat presentations is closed under composition, and the class of cogalois *cn*-extensions is not, as can be shown.

Appendix: A finiteness result

Let, as always, F/k be a finite extension of fields. Since we are mainly interested in coseparable extensions, the only obstruction that might prevent F/k from being cogalois is that $\mathrm{Cog}(F/k)$ may become too large. This motivates the following example and subsequent theorem:

Example. Let $F=\mathbb{Q}(\exp(2\pi \mathrm{i}/2^n))_{n\in\mathbb{N}}$, $k=F\cap\mathbb{R}$. Then $[F:k]=2$ and $\mathrm{Cog}(F/k)$ is countably infinite.

Idea of proof. Show $F=k(\mathrm{i})$, $\mu(k)=\{\pm 1\}$, and $\mu(F)$ is infinite. (μ denotes the set of roots of unity.)

Theorem. *If k is a number field, then* $\mathrm{Cog}(F/k)$ *is finite.*

Remark. If $F=k(\alpha_1,\dots,\alpha_s)$ with $\alpha_i^{n_i}\in \dot{k}$ and $[F:k]=n_1\cdot\cdots\cdot n_s$, then the theorem is a consequence of Theorem A in [7].

Proof of the Theorem. If α is a homomorphism of abelian groups, denote the torsion part of $\mathrm{cok}(\alpha)$ by $C(\alpha)$. If the range of α is finitely generated, then $C(\alpha)$ is finitely generated and torsion, so it is finite. If

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

is exact and commutative, then we have the implications

(i) γ injective, $C(\alpha)$ finite, $C(\gamma)$ finite $\Rightarrow C(\beta)$ finite;

(ii) β injective, $\ker(\gamma)$ finite, $C(\beta)$ finite $\Rightarrow C(\alpha)$ finite.

(The verification of these uses the snake lemma.)

Now we apply (ii) to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Prin}(k) & \longrightarrow & \mathrm{Div}(k) & \longrightarrow & \mathrm{Cl}(k) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow h & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Prin}(F) & \longrightarrow & \mathrm{Div}(F) & \longrightarrow & \mathrm{Cl}(F) & \longrightarrow & 0 \end{array}$$

To do this, we need $C(h)$ finite. We get this by decomposing h into

$$h_{\mathrm{ram}}: \mathrm{Div}_{\mathrm{ram}}(k) \to \mathrm{Div}_{\mathrm{ram}}(F),$$

$$h_{\mathrm{un}}: \mathrm{Div}_{\mathrm{un}}(k) \to \mathrm{Div}_{\mathrm{un}}(F),$$

where ram stands for 'ramified in F/k' and un stands for 'unramified in F/k'. One has to check that $\mathrm{cok}(h_{\mathrm{un}})$ has no torsion at all, and one uses that $\mathrm{Div}_{\mathrm{ram}}(F)$ is finitely generated. Now (ii) yields that $C(f)$ is finite.

Apply (i) to the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U(k) & \longrightarrow & \dot{k} & \longrightarrow & \mathrm{Prin}(k) & \longrightarrow & 0 \\ & & \downarrow j & & \downarrow & & \downarrow f & & \\ 1 & \longrightarrow & U(F) & \longrightarrow & \dot{F} & \longrightarrow & \mathrm{Prin}(F) & \longrightarrow & 0 \end{array}$$

This is possible since f is injective, $C(f)$ is finite by the previous step, and $C(j)$ is finite. ($U(-)$ denotes the unit group of the maximal order.) The result is that the torsion part of $\dot{F}/\dot{k}$ is finite, and this proves the theorem.

References

[1] E. Artin, Galois Theory, Notre Dame Math. Lectures (Notre Dame, 1948).

[2] S.-U. Chase and M. Sweedler, Hopf Algebras and Galois Theory, Lecture Notes in Math. 97 (Springer, Berlin, 1969).

[3] I. Kaplansky, Fields and Rings (Chicago University Press, Chicago, 1969).

[4] S. MacLane, Homology, Grundlehren der Mathematik 114 (Springer, Berlin, 1963).

[5] M. Suzuki, Structure of a Group and the Structure of its Lattice of Subgroups, Ergebnisse der Mathematik (Springer, Berlin, 1956).

[6] D. Gay and W.Y. Vélez, The torsion group of a radical extension, Pacific J. Math. 92 (1981) 317-3227.

[7] M.A. de Orozco and W.Y. Vélez, The lattice of subfields of a radical extension, J. Number Theory 15 (1982) 388–405.