The Bulletin of Symbolic Logic
Volume 16, Number 2, June 2010

AN INVITATION TO MODEL-THEORETIC GALOIS THEORY

ALICE MEDVEDEV AND RAMIN TAKLOO-BIGHASH

Abstract. We carry out some of Galois' work in the setting of an arbitrary first-order theory T. We replace the ambient algebraically closed field by a large model $\mathcal{M}$ of T, replace fields by definably closed subsets of $\mathcal{M}$, assume that T codes finite sets, and obtain the fundamental duality of Galois theory matching subgroups of the Galois group of L over F with intermediate extensions $F \leq K \leq L$. This exposition of a special case of [10] has the advantage of requiring almost no background beyond familiarity with fields, polynomials, first-order formulae, and automorphisms.

§1. Introduction. Two hundred years ago, Évariste Galois contemplated symmetry groups of solutions of polynomial equations, and Galois theory was born. Thirty years ago, Saharon Shelah found it necessary to work with theories that *eliminate imaginaries*; for an arbitrary theory, he constructed a canonical definitional expansion with this property in [15]. Poizat immediately recognized the importance of a theory already having this property in its native language; indeed, he defined "elimination of imaginaries" in [10]. It immediately became clear (see [10]) that much of Galois theory can be developed for an arbitrary first-order theory that eliminates imaginaries. This model-theoretic version of Galois theory can be generalized beyond finite or even infinite algebraic extensions, and this can in turn be useful in other algebraic settings such as the study of Galois groups of polynomial differential equations (already begun in [10]) and linear difference equations. On a less applied note, it is possible to bring further ideas into the model-theoretic setting, as is done in [9] for the relation between Galois cohomology and homogeneous spaces.

Here we rewrite parts of Galois' work in the language of model theory, a special case of [10]. Like Galois, we only treat finite extensions, while [10] addresses finitely-generated infinite extensions, including those generated by a solution of a differential equation. A nice exposition of the more general

Received September 22, 2009.

We thank the anonymous referee and John Baldwin, the editor, for their careful reading and many suggestions. The second author's work is partially supported by NSF grant DMS-0701753 and a research grant from the University of Illinois at Chicago.

1079-8986/10/1602-0004/$1.90

theory, as well as all the model-theoretic prerequisites, can be found in [11]. This paper is the result of collaboration between a number theorist who wanted to learn model theory, and a logician who wanted to remember Galois theory. As such, it is entirely elementary in both algebra and logic, and should be accessible to anyone with any undergraduate background in both. It can also motivate an algebraist to learn a little bit of logic, or enlighten a logician about a bit of algebra. In the interest of this accessibility, we do not give a proper treatment to elimination of imaginaries, and do not describe the construction, for a fixed theory T, of the definitional expansion T^{eq} that eliminates imaginaries. That would require multisorted logic, which, though no harder than the usual one-sorted kind, is rarely taught in introductory courses. Before we launch into the details, let us say which parts of Galois theory we replicate, and which are lost.

We see fields as definably-closed substructures of models of the theory of algebraically closed fields, rather than as models of the theory of fields. This is necessary because otherwise it may be impossible to amalgamate several finite extensions into a normal extension, and indeed it is not even clear what it would mean for an extension to be normal. Thus not every first-order theory can play the role of the theory of fields. In this paper, we define the basic Galois-theoretic notions for an arbitrary theory in place of the theory of algebraically closed fields. However, the fundamental duality of Galois theory requires a harmless technical condition, namely coding finite sets (a special case of elimination of imaginaries). We fix an arbitrary theory T; where Galois worked inside the complex numbers, we work inside a sufficiently saturated model $\mathcal{M}$ of T, as is usual in modern model theory. Thus, all of our models are elementary submodels of $\mathcal{M}$ and all of our sets are subsets of $\mathcal{M}$.

Here are the parts of Galois theory that we replicate. We define the *degree* of an extension, the *automorphism group* of an extension, and *splitting* and *normal* extensions. For a normal extension $F \leq L$, we prove the fundamental duality between intermediate extensions $F \leq K \leq L$ and subgroups of the Galois group of L over F. Next, we show that K is normal over F if and only if the corresponding subgroup is normal. In this case the Galois group of K over F is the appropriate quotient group.

Here are the parts of Galois theory that one cannot hope to have in this generality. Our language may have no function symbols, and our theory may not admit quantifier elimination, so we must replace polynomials by arbitrary first-order formulae. Similarly, in our setting an extension L of K need not be a K-vector space. Indeed, there is no reason to have a definable bijection between L and some cartesian power of K. This rules out the possibility of defining the degree of an extension in terms of the dimension of a vector space, and precludes norms, traces, characters, and discriminants. The conceptual interpretation of the solvability of the Galois group is also lost, as there is no analog of radicals, and no conceptual characterization of cyclic extensions.

Let us now actually define all these words and prove these statements.

§2. The fundamental duality.

Notation:

- We work in a κ-saturated model $\mathcal{M}$ of T; we say that a subset $A \subset \mathcal{M}$ is *small* if $|A| < \kappa$.
- Given an L-formula $\phi(x, y)$ and a tuple $a \in \mathcal{M}$, we say that another tuple $b \in \mathcal{M}$ is a *solution* of $\phi(a, y)$ if $\mathcal{M} \models \phi(a, b)$.
- Given $A \subset \mathcal{M}$, $L(A)$ is the language L augmented by new constant symbols, one for each element of A; we naturally expand $\mathcal{M}$ to an $L(A)$-structure by interpreting the new constant symbols as the corresponding elements of A.
- For a substructure $B \leq \mathcal{M}$ and a subset $A \subset B$, we denote by $\mathrm{Aut}(B/A)$ the group of *partial elementary* maps from B to B fixing A pointwise. (A partial elementary map preserves *all* first-order properties, unlike a partial isomorphism, which only preserves atomic formulae.)
- Unless otherwise specified, letters may denote finite tuples. Thus $a \in A$ should be read as "a is a tuple of elements of A."

Definition 1. *Given a small $A \subset \mathcal{M}$ and a tuple $b \in \mathcal{M}$, we say that $b \in \mathrm{acl}(A)$ (b is algebraic over A, or b is in the algebraic closure of A) if there is an $L(A)$-formula $\phi(y)$ such that b is one of finitely many solutions of $\phi(y)$. If b is the* only *solution of $\phi(y)$, we say that $b \in \mathrm{dcl}(A)$ (b is definable over A, or b is in the definable closure of A).*

If in addition there is no $L(A)$-formula $\psi(y)$ such that $\psi(y)$ still has b as a solution and has fewer solutions than $\phi(y)$, we call $\phi(y)$ an irreducible formula of b over A, *denoted* $\mathrm{irr}(b/A)$.

Given a small $A \subset \mathcal{M}$ and a tuple $b \in \mathcal{M}$, we define $\mathcal{O}(b/A)$ to be the orbit of b under $\mathrm{Aut}(\mathcal{M}/A)$.

Given $b \in \mathrm{acl}(A)$, we define the degree of b over A *to be* $\deg(b/A) := |\mathcal{O}(b/A)|$.

Clearly, $\mathrm{irr}(b/A)$ exists for any $b \in \mathrm{acl}(A)$; although many formulae may fit this definition, they all have the same solution set; so we often abuse notation and speak of *the* formula $\mathrm{irr}(b/A)$. Note also $\mathrm{irr}(b/A)$ is equivalent to $\mathrm{irr}(b/\mathrm{dcl}(A))$. It is easy to check that acl and dcl are indeed closure operators on subsets of $\mathcal{M}$. It is well-known (and easy to show) that $b \in \mathrm{acl}(A)$ if and only if $\mathcal{O}(b/A)$ is finite, and in that case $\mathcal{O}(b/A)$ is the solution set of $\mathrm{irr}(b/A)$, so the degree of b over A is the number of solutions of $\mathrm{irr}(b/A)$. For fields in characteristic zero, this degree is precisely the degree of the usual Galois theory, while in positive characteristic it is the separable degree. It is also clear that the degree is preserved under interdefinability over A, that is $\deg(c/A) = \deg(b/A)$ for any tuple $c \in \mathrm{dcl}(Ab)$ such that $b \in \mathrm{dcl}(Ac)$, which allows us to define the degree of a finite extension.

Definition 2. *Given* $A \subset B \subset \mathcal{M}$, *we say that* B *is a* finite extension of A *if there is a tuple* b *of elements of* $B \cap \operatorname{acl}(A)$ *such that* $B \subset \operatorname{dcl}(Ab)$; *we say that* b generates B over A; *we define the* degree of B over A *to be* $\deg(B/A) := \deg(b/A)$.

If in addition $\mathcal{O}(c/A) \subset B$ *for every tuple* $c \in B$, *we say that* B *is a* normal extension of A. *If there is some* $b \in B$ *such that* $\mathcal{O}(b/A) \subset B$ *and* $B \subset \operatorname{dcl}(A \cup \mathcal{O}(b/A))$, *we say that* B *is the* splitting extension of $\operatorname{irr}(b/A)$ over A.

Lemma 3. *A definably closed splitting extension is normal.*

Proof. Let $B = \operatorname{dcl}(B)$ be the splitting extension of $\operatorname{irr}(b/A)$ over A, that is, $B = \operatorname{dcl}(A \cup \mathcal{O}(b/A))$. Now B must be $\operatorname{Aut}(\mathcal{M}/A)$-invariant because $\mathcal{O}(b/A)$ is. Therefore it contains any $\operatorname{Aut}(\mathcal{M}/A)$-orbit it intersects. ⊣

Lemma 4. *Degrees of finite extensions multiply in towers. That is, if* $A \subset B \subset C$ *are finite extensions, then* $\deg(C/A) = \deg(C/B) \cdot \deg(B/A)$.

Proof. Let b generate B over A, and let c generate C over B. Clearly, the concatenation bc generates C over A. We need to show that $|\mathcal{O}(bc/A)| = |\mathcal{O}(b/A)| \cdot |\mathcal{O}(c/B)|$. For $d \in \mathcal{O}(b/A)$, let

$$S_d := \{(d, \sigma(c)) \mid \sigma \in \operatorname{Aut}(\mathcal{M}/A) \text{ and } \sigma(b) = d\}$$

Clearly $\mathcal{O}(bc/A) = \cup_{d \in \mathcal{O}(b/A)} S_d$ is a disjoint union of $\deg(b/A)$-many sets S_d. Since $S_b = \{(b, \sigma(c)) \mid \sigma \in \operatorname{Aut}(\mathcal{M}/Ab)\}$, it is the same size as $\mathcal{O}(c/B)$. It suffices to show that $|S_d| = |S_b|$ for all $d \in \mathcal{O}(b/A)$. This is true because the size of S_d is a definable property of d: if $\phi(y, z)$ is the $L(A)$-formula such that $\phi(b, z) = \operatorname{irr}(c/Ab)$, then b satisfies $\psi(y) := \exists_{!n} z\, \phi(y, z)$, and so all $d \in \mathcal{O}(b/A)$ must satisfy it too. If $\theta(y) = \operatorname{irr}(b/A)$, it is clear that $\operatorname{irr}(bc/A) = \theta(y) \wedge \phi(y, z)$. ⊣

Lemma 5. *If* $B = \operatorname{dcl}(Ab)$ *is a finite extension of* A, *then* $|\operatorname{Aut}(B/A)| = |B \cap \mathcal{O}(b/A)|$.

Proof. It suffices to construct a bijection between the two sets of allegedly the same size. Let $f\colon \operatorname{Aut}(B/A) \to (B \cap \mathcal{O}(b/A))$ be defined by $f(\sigma) := \sigma(b)$. If $f(\sigma) = f(\tau)$, then $\sigma(b) = \tau(b)$, and so $\sigma \circ \tau^{-1}$ is identity on $\operatorname{dcl}(Ab) = B$. Thus f is injective. Given some $b' \in B \cap \mathcal{O}(b/A)$ let $\sigma \in \operatorname{Aut}(\mathcal{M}/A)$ be such that $\sigma(b) = b'$. Now

$$\sigma(B) = \sigma(\operatorname{dcl}(Ab)) = \operatorname{dcl}(\sigma(Ab)) = \operatorname{dcl}(A\sigma(b)) = \operatorname{dcl}(Ab') \subset B$$

is a definably closed subset of B containing A of the same degree over A as B. Thus $\sigma(B) = B$ by the previous lemma, so $\sigma|_B = f^{-1}(b')$ and f is surjective. ⊣

Corollary 6. *For a finite extension* $B \supset A$, $\deg(B/A) = |\operatorname{Aut}(B/A)|$ *if and only if* B *is a normal extension of* A.

Proof. Let $b \in B \cap \operatorname{acl} A$ be such that $B \subset B' := \operatorname{dcl}(Ab)$. Suppose that B is a normal extension of A. Then $\deg(B/A) = \deg(B'/A) = |\mathcal{O}(b/A)|$ by definition, and $|\mathcal{O}(b/A)| = |\operatorname{Aut}(B'/A)|$ by the last lemma. It suffices to show that the restriction map from $\operatorname{Aut}(B'/A)$ to $\operatorname{Aut}(B/A)$ is well-defined and bijective. Since any automorphism of B can be extended to an automorphism of B' (and indeed of all of $\mathcal{M}$), the restriction is surjective. Since B is normal, it is clearly invariant under automorphisms. Since $B' = \operatorname{dcl}(Ab)$, an automorphism $\sigma \in \operatorname{Aut}(B'/A)$ is completely determined by $\sigma(b)$ and a fortiori by the restriction of σ to B, so that restriction is injective.

Note that any automorphism $\sigma \in \operatorname{Aut}(B/A)$ is determined by $\sigma(b)$, so

$$|\operatorname{Aut}(B/A)| \leq |B \cap \mathcal{O}(b/A)| \leq |\mathcal{O}(b/A)|$$

with the last inequality strict if B is not a normal extension of A. $\dashv$

Note that if $A \subset B \subset C$ and C is normal over A, then C is also normal over B, as orbits of $\operatorname{Aut}(C/B)$ are subsets of orbits of $\operatorname{Aut}(C/A)$.

COROLLARY 7. *If $A \subset B \subset C$ and B and C are normal over A, then $|\operatorname{Aut}(C/A)| = |\operatorname{Aut}(C/B)| \cdot |\operatorname{Aut}(B/A)|$ and in fact*

$$0 \to \operatorname{Aut}(C/B) \to \operatorname{Aut}(C/A) \to \operatorname{Aut}(B/A) \to 0$$

is exact, so $\operatorname{Aut}(C/B)$ is a normal subgroup of $\operatorname{Aut}(C/A)$.

PROOF. Naturally, $\operatorname{Aut}(C/B) \subset \operatorname{Aut}(C/A)$. Since B is normal, it is $\operatorname{Aut}(C/A)$-invariant, so restriction gives a surjective homomorphism $\operatorname{Aut}(C/A) \to \operatorname{Aut}(B/A)$ whose kernel clearly is $\operatorname{Aut}(C/B)$. $\dashv$

DEFINITION 8. *Suppose that $C = \operatorname{dcl}(C)$ is a finite extension of $A = \operatorname{dcl}(A)$, and $G := \operatorname{Aut}(C/A)$. If H is a subgroup of G, we let*

$$\operatorname{Fix}(H) := \{c \in C \mid \forall h \in H\, h(c) = c\}$$

be the set of elements of C fixed pointwise by every element of H.

If $A \subset B \subset C$, we let $\operatorname{Fix}(B) := \{h \in G \mid \forall b \in B\, h(b) = b\}$ be the subgroup of G of elements that fix B pointwise.

Note that for any subgroup H, the set $\operatorname{Fix}(H)$ is definably closed.

LEMMA 9. *If $A \subset B \subset C$ are definably closed, and C is a normal extension of A, then $H := \operatorname{Aut}(C/B)$ is normal in $G := \operatorname{Aut}(C/A)$ if and only if B is a normal extension of A.*

PROOF. The last corollary proves one direction, so we need to prove the other. Suppose that B is not normal, that is there is some $b \in B$ with $\mathcal{O}(b/A) \not\subset B$. Since B is definably closed, and $\mathcal{O}(b/A)$ is B-definable (since it is A-definable), there must be at least two elements $c, d \in \mathcal{O}(b/A)$ not in B, and we may further assume that $d \in \mathcal{O}(c/B)$. We now find $h \in H$ and some $g \in G$ such that $g^{-1}hg \notin H$. We will take h witnessing $d \in \mathcal{O}(c/B)$, that is such that $h(c) = d$. We will take g witnessing that $c \in \mathcal{O}(b/A)$, that is such that $g(b) = c$. Now $h(g(b)) = h(c) = d$, and since $d \neq c$, $g^{-1}(d) \neq g^{-1}(c) = b$, so $g^{-1}hg(b) \neq b$, so $g^{-1}hg(b) \notin H = \operatorname{Aut}(C/B)$, as wanted. $\dashv$

We now define a special case of elimination of imaginaries that is necessary for the fundamental duality of Galois theory. Recall that $\mathcal{M}$ is a monster model of our theory T.

Definition 10. *We say that T* codes finite sets of tuples *if for any $n \in \mathbb{N}$ and for any finite $F \subset \mathcal{M}^n$ there is some tuple b such that for any automorphism $\sigma \in \mathrm{Aut}(\mathcal{M})$ we have $\sigma(b) = b$ if and only if $\sigma(F) = F$. We call b the* code *of F.*

Full elimination of imaginaries is equivalent to the same condition for all, not necessarily finite, definable (with parameters) sets F. For example from algebraic geometry, the code of a variety is (the finite tuple of generators of) its field of definition. It is clear that the code b of F is well-defined up to interdefinability, and that if F is A-definable, then $b \in \mathrm{dcl}(A)$. We only use the coding of finite sets of tuples once, where the tuple is the generator of a finite extension.

It is well-known that the theory of algebraically closed fields codes finite sets of tuples: a set of m n-tuples is coded by the tuple of elementary multi-symmetric polynomials. Let S be a set of m n-tuples of variables; a polynomial P in all these variables is multi-symmetric in S if P is invariant under permutations of S; P is elementary multi-symmetric if it is monic, homogeneous, of degree at most m in each variable. For example, $(a+b+c, ab+ac+bc, abc)$ is a code of $\{a, b, c\}$ and $(a+c, ac, b+d, bd, ad+bc)$ is a code for $\{(a, b), (c, d)\}$. A complete proof would be neither short nor beautiful.[1]

Here is an example of a theory that fails to code finite sets. In it, there is no Galois correspondence between subgroups of $\mathrm{Aut}(C/A)$ and intermediate definably closed sets B with $A \subset B \subset C$.

Example 11. *Take a language L with two binary relations R and S, and let $\mathcal{M}$ be an L-structure with an infinite universe containing points a, b, c, and d. Let*

$$R^{\mathcal{M}} := \{(a, b), (b, a), (c, d), (d, c)\}$$

and

$$S^{\mathcal{M}} := \{(a, c), (c, a), (b, d), (d, b)\}.$$

Note that this theory does not code finite sets; in particular, the unordered sets $\{a, b\}$ and $\{c, d\}$ are not interdefinable with any tuples. Let A be anything disjoint from $\{a, b, c, d\}$; then $C := \{a, b, c, d\} \cup A$ is a finite extension of A. Then $\mathrm{Aut}(C/A)$ contains four elements: an automorphism may fix all four

[1] "Dans la troisième section, il faut donc prouver cette élimination des imaginaires pour les corps algébriquement clos; l'argument essential est un exercice sur les fonctions symétriques (Lemme 5) dont l'auteur, sans doute par manque de culture, n'a pas trouvé de traces dans la littérature; il doit s'agir d'un résultat "bien connu", un de ceux dont on n'ose publier une démonstration qu'en cas d'absolue nécessité." [10].

points, or it may switch two disjoint pairs of them, for example switching a with d and b with c. However, there are no definably closed B with $A \subset B \subset C$ except for A and C.

That is the only obstruction.

THEOREM 12. *Suppose that T codes finite sets, that $C = \mathrm{dcl}(C)$ is a normal extension of $A = \mathrm{dcl}(A)$, and $G := \mathrm{Aut}(C/A)$. Then there is a bijection between subgroups of G and intermediate definably closed extensions given by associating a subgroup H to the set $\mathrm{Fix}(H)$, and a set B to the subgroup $\mathrm{Fix}(B)$.*

PROOF. We need to show that $\mathrm{Fix}(\mathrm{Fix}(H)) = H$ for any H, and that $\mathrm{Fix}(\mathrm{Fix}(B)) = B$ for any B. The proof relies on the fact that the restriction map $\mathrm{Aut}(\mathcal{M}/A) \to \mathrm{Aut}(C/A)$ is well-defined and surjective.

The second part is easier. Clearly, it suffices to show that $\mathrm{Fix}(\mathrm{Fix}(B)) \subset \mathrm{dcl}(B)$. Suppose that $c \notin \mathrm{dcl}(B)$; then there is some automorphism $\sigma \in \mathrm{Aut}(\mathcal{M}/B)$ such that $\sigma(c) \neq c$. Abusing notation we also denote the restriction of σ to C by $\sigma \in \mathrm{Aut}(C/A)$. Since $\sigma \in \mathrm{Fix}(B)$ but $\sigma(c) \neq c$, this σ witnesses that $c \notin \mathrm{Fix}(\mathrm{Fix}(B))$.

For the first part, it suffices to find some tuple b of elements of $\mathrm{Fix}(H)$ such that $g(b) \neq b$ for any $g \notin H$. This b will be a code of the orbit of a generator of C/A under H. Let c be such that $C = \mathrm{dcl}(Ac)$, let $F := \{h(c) \mid h \in H\}$, and let b be the code of F. Note that H acts (faithfully transitively) on F, so in particular $h(F) = F$ for all $h \in H$, so the entries of b are in $\mathrm{Fix}(H)$. On the other hand, take some $g \in G$ that is not in H. Note that $g(c) = h(c)$ implies that $g = h$, so $g(c) \notin F$. But $c \in F$, so $g(c) \in g(F)$. Thus, g does not leave F invariant, and therefore does not fix b the code of F. $\dashv$

§3. Further developments.

Since Shelah's invention of imaginaries in 1978 and Poizat's seminal paper [10] in 1983, much more has been done with automorphism groups in model theory. Already [10] speaks about the absolute Galois group of A acting not only on the elements of the algebraic closure $\bar{A}$ (which correspond to the algebraic types over $\bar{A}$) but also on the whole Stone space $S(\bar{A})$ of types over $\bar{A}$.

Sometimes, the Galois group appears as a definable *binding group* inside the model. This already occurs in the earliest application of this abstract theory, to linear differential equations in [10]. When anything remotely like this happens, it is extremely useful, for example allowing one to extract a definable field out of a definable group action. See [12] or [8] for an introduction to binding groups. In some sense, this gives a definable representation of the Galois group.

Algebraists have not been idle either: Galois would hardly recognize the Galois theory in modern algebra textbooks. Galois Theory was fully developed by Weber [17], Steinitz [16], and Artin [1]. The Galois theory of infinite extensions was initiated by Krull [6]. In these developments a central role is played by the simple observation that any extension field of finite degree is a finite dimensional vector space over the ground field. This opens the way to import ideas and techniques from linear algebra. Of course none of this happens on our level of generality. The notion of Krull topology, however, carries over to our setting with little modification. Weil [18] invented universal domains, of which our monster models are a natural generalization, and also introduced *fields of definition*, which have an exact analog in *canonical parameters* of definable sets. Here we should also mention the developments growing out of the introduction of Galois theory in the setting of commutative rings [2], as well as Rasala's Inseparable Splitting Theory [13], as notable progress in the algebraic aspects of the subject.

Many of the connections of Galois theory to number theory and algebraic geometry are via homological algebra. For example, Galois cohomology, at least in the commutative setting, is now an important tool in algebraic number theory and class field theory (see e.g., [7]). Cohomological methods combined with representation theoretic, analytic, and algebro-geometric techniques have produced astonishing results in number theory (e.g., [19] and [5]). Non-abelian Galois cohomology is considerably more difficult to handle, and for that reason has not found much popularity among the mathematical public; though, the non-commutative H^1 is now routinely used in questions of classification and forms (see e.g., [14]). Giraud's book [4] contains a comprehensive study of general non-abelian cohomology. Some of these notions have been put into the language of model theory in [9] and most recently in [3]. Further exploration of the connections between model theory and higher non-abelian cohomology seems rather inevitable, as no land this accessible and this pristine can keep off intruders for long.

REFERENCES

[1] EMIL ARTIN, ***Galois Theory***, Notre Dame Mathematical Lectures, no. 2, University of Notre Dame, Notre Dame, Ind., 1942, edited and supplemented with a section on applications by Arthur N. Milgram.

[2] S. U. CHASE, D. K. HARRISON, and ALEX ROSENBERG, *Galois theory and Galois cohomology of commutative rings*, ***Memoirs of the American Mathematical Society***, vol. 52 (1965), pp. 15–33.

[3] DAVID M. EVANS and ELISABETTA PASTORI, *Second cohomology groups and finite covers*, 2009.

[4] JEAN GIRAUD, ***Cohomologie non abélienne***, Die Grundlehren der mathematischen Wissenschaften, Band 179, Springer-Verlag, Berlin, 1971.

[5] MICHAEL HARRIS and RICHARD TAYLOR, ***The geometry and cohomology of some simple Shimura varieties***, Annals of Mathematics Studies, vol. 151, Princeton University Press, Princeton, NJ, 2001, with an appendix by Vladimir G. Berkovich.

[6] WOLFGANG KRULL, *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, ***Mathematische Annalen***, vol. 100 (1928), no. 1, pp. 687–698.

[7] JÜRGEN NEUKIRCH, ***Algebraic number theory***, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag,

Berlin, 1999, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.

[8] ANAND PILLAY, ***Geometric stability theory***, Oxford Logic Guides, vol. 32, The Clarendon Press Oxford University Press, New York, 1996.

[9] ———, *Remarks on Galois cohomology and definability*, ***The Journal of Symbolic Logic***, vol. 62 (1997), no. 2, pp. 487–492.

[10] BRUNO POIZAT, *Une théorie de Galois imaginaire*, ***The Journal of Symbolic Logic***, vol. 48 (1983), no. 4, pp. 1151–1170 (1984).

[11] ———, ***A course in model theory***, Universitext, Springer-Verlag, New York, 2000, translated from the French by Moses Klein and revised by the author.

[12] ———, ***Stable groups***, Mathematical Surveys and Monographs, vol. 87, American Mathematical Society, Providence, RI, 2001, translated from the 1987 French original by Moses Gabriel Klein.

[13] RICHARD RASALA, *Inseparable splitting theory*, ***Transactions of the American Mathematical Society***, vol. 162 (1971), pp. 411–448.

[14] I. SATAKE, ***Classification theory of semi-simple algebraic groups***, Lecture Notes in Pure and Applied Mathematics, vol. 3, Marcel Dekker Inc., New York, 1971, with an appendix by M. Sugiura, notes prepared by Doris Schattschneider.

[15] SAHARON SHELAH, ***Classification theory and the number of nonisomorphic models***, Studies in Logic and the Foundations of Mathematics, vol. 92, North-Holland Publishing Co., Amsterdam, 1978.

[16] ERNST STEINITZ, ***Algebraische Theorie der Körper***, Chelsea Publishing Co., New York, N. Y., 1950.

[17] H. WEBER, *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*, ***Mathematische Annalen***, vol. 43 (1893), no. 4, pp. 521–549.

[18] ANDRÉ WEIL, ***Foundations of algebraic geometry***, American Mathematical Society Colloquium Publications, vol. 29, American Mathematical Society, New York, 1946.

[19] ANDREW WILES, *Modular elliptic curves and Fermat's last theorem*, ***Annals of Mathematics. Second Series***, vol. 141 (1995), no. 3, pp. 443–551.

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE
UNIVERSITY OF ILLINOIS AT CHICAGO
322 SCIENCE AND ENGINEERING OFFICES (M/C 249)
851 S. MORGAN STREET
CHICAGO, IL 60607-7045, USA
E-mail: alice@math.uic.edu
E-mail: rtakloo@math.uic.edu