

Introduction to the Lascar Group

Martin Ziegler*

June 13, 2001

1 Introduction

The aim of this article is to give a short introduction to the Lascar Galois group $\text{Gal}_L(T)$ of a complete first order theory T . We prove that $\text{Gal}_L(T)$ is a quasicompact topological group in section 5. $\text{Gal}_L(T)$ has two canonical normal closed subgroups: $\Gamma_1(T)$, the topological closure of the identity, and $\text{Gal}_L^0(T)$, the connected component. In section 6 we characterize these two groups by the way they act on bounded hyperimaginaries. In the last section we give examples which show that every compact group occurs as a Lascar Galois group and an example in which $\Gamma_1(T)$ is non-trivial.

None of the results, except possibly Corollary 26, are new, but some technical lemmas and proofs are. In particular, the treatment of the topology of $\text{Gal}_L(T)$ in sections 4 and 5 avoids ultraproducts, by which the topology was originally defined in [6]. Most of the theory expounded here was taken from that article, and the more recent [7], [4] and [2].

I thank Katrin Tent for reading the manuscript carefully, Markus Tressl, who found a serious mistake in an earlier version, and Anand Pillay, who helped me with the proof of Theorem 23.

2 The group

We fix a complete theory T . Let \mathbb{C} be a saturated¹ model of T , of cardinality larger than $2^{|T|}$, and let $\text{Aut}(\mathbb{C})$ its automorphism group. The subgroup $\text{Aut}_L(\mathbb{C})$ generated by all point-wise stabilizers $\text{Aut}_M(\mathbb{C})$ of elementary² submodels M is called the group of *Lascar strong* automorphisms. $\text{Aut}_L(\mathbb{C})$ is a

*Partially supported by the Mittag-Leffler Institute, Stockholm

¹ T may not have saturated models. In this case we take for \mathbb{C} a *special* model (see [3] Chapter 10.4) of T and use the $\text{cf}|\mathbb{C}|$ instead of $|\mathbb{C}|$. Especially we assume that $\text{cf}|\mathbb{C}| > 2^{|T|}$.

²In the sequel *submodel* will always mean *elementary submodel*.

normal subgroup of $\text{Aut}(\mathbb{C})$. The quotient is the *Lascar (Galois) group* of \mathbb{C} :

$$\text{Gal}_L(\mathbb{C}) = \text{Aut}(\mathbb{C})/\text{Aut}_L(\mathbb{C}).$$

We will show that $\text{Gal}_L(\mathbb{C})$ does not depend on the choice of \mathbb{C} .

Lemma 1 *Let M and N be two small³ submodels of \mathbb{C} and f an automorphism. Then the class of f in $\text{Gal}_L(\mathbb{C})$ is determined by the type of $f(M)$ over N .*

PROOF: Let $(m_i)_{i \in I}$ be an enumeration of M . By the type of $f(M)$ over N we mean the type of the infinite tuple $(f(m_i))_{i \in I}$ over N . This is a type in variables $(x_i)_{i \in I}$. We denote by $S_I(N)$ the set of all such types over N .

Let $g(M)$ have the same type over N as $f(M)$. Choose an automorphism s which fixes N and maps $f(M)$ to $g(M)$. Then s is a Lascar strong automorphism, as is $t = (sf)^{-1}g$, which fixes M . Now we see that $g = sft$ and f have the same class in $\text{Gal}_L(\mathbb{C})$. \square

Two possibly infinite tuples a and b from \mathbb{C} are said to have the same *Lascar strong type* iff $f(a) = b$ for a Lascar strong automorphism f .

Lemma 2 *a and b have the same Lascar strong type iff there is a sequence of tuples $a = a_0, \dots, a_n = b$ and a sequence of small submodels N_1, \dots, N_n such that, for each i , a_{i-1} and a_i have the same type over N_i .*

PROOF: Clear \square

Corollary 3 *a and b have the same Lascar strong type in \mathbb{C} if they have the same Lascar strong type in an elementary extension of \mathbb{C} .*

PROOF: If a_0, \dots, N_n exist in an elementary extension of \mathbb{C} , we find by saturation in \mathbb{C} a sequence a'_0, \dots, N'_n which has the same type over ab as a_0, \dots, N_n . This sequence shows that a and b have the same Lascar strong type in \mathbb{C} . \square

Theorem 4 ([6]) $\text{Gal}_L(\mathbb{C})$ *depends only on T and not on the choice of \mathbb{C} .*

PROOF: If \mathbb{C}' is another big saturated model of T we can assume that \mathbb{C}' is an elementary extension of \mathbb{C} and of larger cardinality. We can extend every automorphism f of \mathbb{C} to an automorphism f' of \mathbb{C}' . Since all such f' differ only by elements of $\text{Aut}_{\mathbb{C}}(\mathbb{C}')$, this defines a homomorphism $\text{Aut}(\mathbb{C}) \rightarrow \text{Gal}_L(\mathbb{C}')$. If f is Lascar strong, f' is Lascar strong as well. Whence we have a well defined natural map

$$\text{Gal}_L(\mathbb{C}) \rightarrow \text{Gal}_L(\mathbb{C}'),$$

³of smaller cardinality than \mathbb{C}

which will turn out to be an isomorphism.

To prove surjectivity, fix an automorphism g of \mathbb{C}' . Choose two small submodels M and N of \mathbb{C} . By saturation we find a submodel M' of \mathbb{C} which has the same type over N as $g(M)$. There is an automorphism f of \mathbb{C} which maps M to M' . Extend f to an automorphism f' of \mathbb{C}' . Then $f'(M)$ and $g(M)$ have the same type over N . Whence, by the last lemma f' and g represent the same element of $\text{Gal}_L(\mathbb{C}')$.

Now assume that $f \in \text{Aut}(\mathbb{C})$ extends to a Lascar strong automorphism f' of \mathbb{C}' . Fix a small submodel M of \mathbb{C} . Then M and $f(M)$ have the same Lascar strong type in \mathbb{C}' , whence also in \mathbb{C} by Corollary 3. So M can be mapped to $f(M)$ by a Lascar strong automorphism of \mathbb{C} . Such an automorphism agrees with f on M , whence f is also strong. This shows that $\text{Gal}_L(\mathbb{C}) \rightarrow \text{Gal}_L(\mathbb{C}')$ is injective. \square

Definition *The Lascar group of T is the quotient*

$$\text{Gal}_L(T) = \text{Aut}(\mathbb{C})/\text{Aut}_L(\mathbb{C}),$$

where \mathbb{C} is any big saturated model of T .

Corollary 5 *The cardinality of $\text{Gal}_L(T)$ is bounded by $2^{|T|}$.*

PROOF: The class of f in $\text{Gal}_L(T)$ is determined by the type of $f(M)$ over N . If M and N are chosen to be of cardinality T , there are at most $2^{|T|}$ possible types. \square

3 Digression: Lascar strong types and thick formulas

Definition *Let $\theta(x, y)$ be a formula in two tuples of variables x and y having the same length. $\theta(x, y)$ is thick, if it has no infinite antichain, that is a sequence of tuples a_0, a_1, \dots such that $\mathbb{C} \models \neg\theta(a_i, a_j)$ for all $i < j$.*

Clearly $\theta(x, y)$ is thick iff there is no indiscernible sequence a_0, a_1, \dots such that $\mathbb{C} \models \neg\theta(a_0, a_1)$. With this description it is easy to see that the intersection of two thick formulas is thick again and that a formulas remains thick if one interchanges the role of x and y .

Lemma 6 *Let $\Theta(x, y)$ be the set of all thick formulas in x and y and let a and b two tuples of the same length. Then the following are equivalent:*

a) $\mathbb{C} \models \Theta(a, b)$

b) a and b belong to an infinite indiscernible sequence.

PROOF: Assume $\mathbb{C} \models \Theta(a, b)$. Then, if $\psi(x, y)$ is satisfied by ab , $\neg\psi$ is not thick, so there is an infinite sequence of indiscernibles a_0, a_1, \dots such that $\psi(a_0, a_1)$ is true. Whence, by compactness, there is one infinite sequence of indiscernibles such that $a_0 a_1$ has the same type as ab .

If conversely a, b are the first two elements of an infinite indiscernible sequence they have to satisfy all thick formulas \square

Lemma 7

1. If $\mathbb{C} \models \Theta(a, b)$, there is a model over which a and b have the same type.
2. If a and b have the same type over some model, the pair ab satisfies the relational product $\Theta \circ \Theta$. I.e. there is a tuple a' such that $\mathbb{C} \models \Theta(a, a')$ and $\mathbb{C} \models \Theta(a', b)$.

PROOF:

1. Let I be an infinite sequence of indiscernibles and M any small model. Then there are indiscernibles I' over M of the same type as I . Whence there is a model M' of the same type as M over which I is indiscernible. Therefore, if a, b are the first elements of some I , they have the same type over some model M' . Now apply Lemma 6.

A more direct proof, which avoids Lemma 6, uses the observation that two sequences a and b of the same length have the same type over a model iff ab satisfies all formulas of the form

$$\exists z \varphi(z) \rightarrow \exists z (\varphi(z) \wedge \bigwedge_{i=1}^n \psi_i(x, z) \leftrightarrow \psi_i(y, z)) \quad (1)$$

for all finite variable tuples z and formulas $\varphi(z), \psi_1(x, z), \dots, \psi_n(x, z)$. All formulas (1) are thick, antichains have length at most 2^n .

2. Assume that a and b have the same type over M . If θ is a thick formula, consider a maximal antichain a_1, \dots, a_n for θ in M . Then, since M is an elementary substructure, a_1, \dots, a_n is also a maximal antichain in \mathbb{C} . Whence $\mathbb{C} \models \theta(a_i, a)$ for some i . Since b has the same type over M , we have $\mathbb{C} \models \theta(a_i, b)$. This proves that for every finite subset Θ_0 of Θ there is an a' such that $\mathbb{C} \models \Theta_0(a', a)$ and $\mathbb{C} \models \Theta_0(a', b)$. This proves the claim using compactness and the observation that Θ defines a symmetric relation. \square

Corollary 8 *The relation of having the same Lascar strong type is the transitive closure of the relation defined by Θ .* \square

Let π be a type defined over the empty set. A formula $\theta(x, y)$ is *thick on π* if θ has no infinite antichain in $\pi(\mathbb{C})$. Let Θ_π be the set of all formulas which are thick over π .

Corollary 9 *Two realizations of π , a and b , have the same Lascar strong type if the pair (a, b) is in the transitive closure of the relation defined by Θ_π .*

PROOF: Assume that a and b have the same type over a model M . The proof of Lemma 7 (1) shows that we can assume that M is ω -saturated. If θ is thick on π , let a_1, \dots, a_n be a maximal antichain for θ in $\pi(M)$. Then, since M is ω -saturated, a_1, \dots, a_n is also maximal in $\pi(\mathbb{C})$. Now proceed as in Lemma 7 (2). \square

4 The topology

Let M and N be two small submodels of \mathbb{C} . Assign to every automorphism f of \mathbb{C} the type of $f(M)$ over N . This defines a surjective map μ from $\text{Aut}(\mathbb{C})$ to $S_M(N)$, the set all types over N of conjugates of M . By Lemma 1 the projection $\text{Aut}(\mathbb{C}) \rightarrow \text{Gal}_L(T)$ factors through μ :

$$\text{Aut}(\mathbb{C}) \xrightarrow{\mu} S_M(N) \xrightarrow{\nu} \text{Gal}_L(T).$$

$S_M(N)$, as a closed subspace of $S_I(N)$, is a boolean space. We give $\text{Gal}_L(T)$ the quotient topology with respect to ν .

To show that this does not depend on the choice of M and N we consider another pair M' and N' . We may assume that $M \subset M'$ and $N \subset N'$. The map $S_{M'}(N') \rightarrow \text{Gal}_L(T)$ then factors as

$$S_{M'}(N') \rightarrow S_M(N) \xrightarrow{\nu} \text{Gal}_L(T),$$

where the first map is restriction of types. Since restriction is continuous and the spaces are compact, $S_M(N)$ carries the quotient topology of $S_{M'}(N')$, which implies that on $\text{Gal}_L(T)$ the two topologies, coming from $S_{M'}(N')$ and $S_M(N)$, are the same.

A quotient of a quasicompact space remains quasicompact. So we have

Lemma 10 *$\text{Gal}_L(T)$ is quasicompact.* \square

Let p and q be types in $S_M(N)$. Two realizations M' and M'' of p and q have the same Lascar strong type iff $\nu(p) = \nu(q)$. Whence, by Corollary 8, the equivalence relation

$$p \approx q \Leftrightarrow \nu(p) = \nu(q)$$

is the transitive closure of the relation D , where $D(p, q)$ holds if p and q have realizations M' and M'' with $\mathbb{C} \models \Theta(M', M'')$.

Lemma 11

1. D is a closed subset of $S_M(N) \times S_M(N)$

2. \approx is a F_σ -set, i.e. a countable union of closed sets.

PROOF:

1. This is clear, because

$$D(p, q) \Leftrightarrow p(x) \cup q(y) \cup \Theta(x, y) \text{ consistent.}$$

2. \approx is the union of all powers

$$D^n = \underbrace{D \circ \dots \circ D}_{n \text{ times}}.$$

So, it suffices to show that all D^i are closed. This follows from the fact that, in compact spaces, the product of two closed relations is closed again. To see this, note that, for binary relations R and S , $R \circ S$ is the projection of $\{(p, q, r) | R(p, q) \wedge S(q, r)\}$ onto the first and third variable. \square

In general the map $S_M(N) \xrightarrow{\nu} \text{Gal}_L(T)$ is not open.⁴ But it has a property that comes close to openness. Define for $p \in S_M(N)$

$$D[p] = \{q \in S_M(N) \mid D(p, q)\}.$$

Lemma 12 *If $D[p]$ is contained in the interior of some subset $O \subset S_M(N)$, then $\nu(p)$ is an inner point of $\nu(O)$.*

PROOF: $D[p]$ is the intersection of all

$$D_\delta[p] = \{q \in S_M(N) \mid p(x) \cup q(y) \cup \{\delta(x, y)\} \text{ consistent}\}, \quad (\delta \in \Theta).$$

By compactness some $D_\delta[p]$ is contained in (the interior of) O .

Claim 1: p is an inner point of $D_\delta[p]$.

Proof: Since δ is thick, there is a finite set $\{H_1, \dots, H_n\}$ of realizations of p such that for every other realization H we have $\mathbb{C} \models \delta(H_i, H)$ for some i . By compactness this is true for every realization H of any p' contained in a small enough neighborhood C of p , which implies that C is contained in $D_\delta[p]$.

After replacing O by $\nu^{-1}(\nu O)$ we can assume that O is closed under \approx (i.e. is a union of \approx -classes.) We set

$$U = \{q \in S_M(N) \mid D_\delta[q] \subset O \text{ for some } \delta \in \Theta\}.$$

⁴If $\text{Aut}(\mathbb{C})$ is endowed with the topology of point-wise convergence, μ becomes continuous (see Lemma 29). If ν were always open, $\text{Aut}(\mathbb{C}) \rightarrow \text{Gal}_L(T)$ would be open too: If a, b are two (finite) tuples, choose N, M in such a way that $a, b \in M = N$. Then the basic open set $\{f \in \text{Aut}(\mathbb{C}) \mid f(a) = b\}$ will be mapped onto an open subset of $S_M(N)$ and whence, by assumption, onto an open subset of $\text{Gal}_L(T)$. Whence, the closedness of $\text{Aut}_L(\mathbb{C})$ would imply that $\text{Gal}_L(T)$ is hausdorff. That this is not true shows one of the examples in [2] ($Th(M^*)$ in Proposition 4.5).

U contains p .

Claim 2: U is closed under \approx .

Proof: Let q be in U , witnessed by $D_\delta[q] \subset O$, and $q \approx r$. Then a realization H of q is mapped by a Lascar strong automorphism f to a realization $f(H) = K$ of r . In order to show that r belongs to U we fix an element r' of $D_\delta[r]$. We have then a realization K' of r' such that $\mathbb{C} \models \delta(K, K')$. Let q' be the type of $H' = f^{-1}(K')$ over M . Since $\mathbb{C} \models \delta(H, H')$, q' belongs to $D_\delta[q]$ and therefore to O . Since $q \approx q'$ and O is closed under \approx , we have $q' \in O$. It follows $D_\delta[r] \subset O$.

Claim 3: U is open.

Proof: U is a subset of the interior of O by Claim 1. Since U is closed under \approx , it is contained in the open set

$$U' = \{q \in S_M(N) \mid D[q] \subset \text{interior}(O)\},$$

which, by compactness, equals

$$U'' = \{q \in S_M(N) \mid D_\delta[q] \subset \text{interior}(O) \text{ for some } \delta \in \Theta\}.$$

But U'' is contained in U , which shows that $U = U'$.

By Claims 2 and 3 the projection of U is an open subset of $\nu(O)$ and contains $\nu(p)$. This completes the proof of Lemma. \square

Corollary 13 *If L is countable, $\text{Gal}_L(T)$ has a countable basis.*

PROOF: If L is countable we can choose countable M and N . $S_M(N)$ has then a countable base, \mathcal{B} . We can assume that \mathcal{B} is closed under finite unions. Let us show that the set of all $\nu(B)^\circ$, ($B \in \mathcal{B}$), is a basis of $\text{Gal}_L(T)$. Let Ω be open and $\alpha \in \Omega$. Choose a preimage p of α and a basic open set B , such that $D[p] \subset B \subset \nu^{-1}(\Omega)$. This is possible, since B is compact and \mathcal{B} closed under finite unions. Then $\nu(B)^\circ \subset \Omega$ is an open neighborhood of p . \square

The following corollary is a reformulation of Corollary 3.5 in [2].

Corollary 14 *Let X be a subset of $\text{Gal}_L(T)$. Then*

$$\overline{X} = \nu(\overline{\nu^{-1}(X)}).$$

PROOF: Since ν is continuous the right hand side lies inside \overline{X} . Let $\nu(p)$ be an element of $\text{Gal}_L(T)$ which does not belong to $\overline{\nu^{-1}(X)}$. Then the whole \approx -class of p , which contains $D[p]$, is disjoint from $\overline{\nu^{-1}(X)}$. By Lemma 12 the complement of $\overline{\nu^{-1}(X)}$ is mapped to a neighborhood of $\nu(p)$, which is disjoint from X . This shows $\nu(p) \notin \overline{X}$. \square

Corollary 15 $\text{Gal}_{\mathbb{L}}(T)$ is hausdorff iff \approx is closed.

PROOF: “ $\text{Gal}_{\mathbb{L}}(T)$ hausdorff $\Rightarrow \approx$ closed” is an easy consequence of the continuity of ν .

Now assume that \approx is closed. Consider two different elements x, y of $\text{Gal}_{\mathbb{L}}(T)$. Since \approx is closed, we can separate each element of $\nu^{-1}(x)$ from each element of $\nu^{-1}(y)$ by a pair of neighborhoods which projects onto disjoint subsets of $\text{Gal}_{\mathbb{L}}(T)$. But $\nu^{-1}(x)$ and $\nu^{-1}(y)$ are compact. This implies that there is one pair of open sets, O and U , which separate $\nu^{-1}(x)$ and $\nu^{-1}(y)$ and have disjoint projections $\nu(O)$ and $\nu(U)$, which are, by the lemma, neighborhoods of x and y . \square

We will see in section 7 (Theorem 28) that $\text{Gal}_{\mathbb{L}}(T)$ need not to be hausdorff.

5 The topological group

Theorem 16 (Lascar) $\text{Gal}_{\mathbb{L}}(T)$ is a topological group.

For the proof we fix again two small submodels M and N and consider the natural mappings

$$\text{Aut}(\mathbb{C}) \xrightarrow{\mu} S_M(N) \xrightarrow{\nu} \text{Gal}_{\mathbb{L}}(T).$$

Lemma 17 *The projections of multiplication*

$$\mathcal{M} = \{(\mu(f), \mu(g), \mu(fg)) \mid f, g \in \text{Aut}(\mathbb{C})\}$$

and of inversion

$$\mathcal{I} = \{(\mu(f), \mu(f^{-1})) \mid f \in \text{Aut}(\mathbb{C})\}$$

are closed subset of $S_M(N) \times S_M(N) \times S_M(N)$ and of $S_M(N) \times S_M(N)$, respectively.

PROOF: We introduce two unary function symbols F and G and express the fact that F are G automorphisms by the $L \cup \{F, G\}$ -theory $A(F, G)$. Then (p, q, r) belongs to \mathcal{M} iff there are functions $f, g : \mathbb{C} \rightarrow \mathbb{C}$ which satisfy the theory

$$B(F, G, p, q, r) = A(F, G) \cup p(F(M)) \cup q(G(M)) \cup r(F(G(M))).$$

Since \mathbb{C} is saturated, $B(F, G, p, q, r)$ can be satisfied in \mathbb{C} if it is consistent with the theory of $\mathbb{C}_{M, N}$. This is a closed condition on p, q, r .

The closedness of \mathcal{I} is similar. \square

The graphs of the multiplication and inversion in $\text{Gal}_L(T)$ are the projections of \mathcal{M} and \mathcal{I} . If $\text{Gal}_L(T)$ is hausdorff, the projections are closed, which, by compactness, implies that multiplication and inversion are continuous in $\text{Gal}_L(T)$.

For the general case we need the following notation: For two subsets of A and B of $S_M(N)$ define

$$A * B = \{r \in S_M(N) \mid (p, q, r) \in \mathcal{M} \text{ for a pair } (p, q) \in A \times B\}.$$

Lemma 18 *If A and B are closed and $A * B$ is contained in the open set W , there are neighborhoods U and V of A and B such that $U * V \subset W$.*

PROOF: Let W' be the complement of W . $A \times B$ is disjoint from the projection C of

$$\mathcal{M} \cap (S_M(N) \times S_M(N) \times W')$$

on the first two coordinates. Since C is closed (and A and B are compact) there are neighborhoods U and V of A and B such that $U \times V$ is disjoint from C . It follows that $U * V \subset W$. \square

We can now prove that multiplication in $\text{Gal}_L(T)$ is continuous. Let $\alpha = \nu(p)$ and $\beta = \nu(q)$ be elements of $\text{Gal}_L(T)$ and Ω an open neighborhood of $\alpha\beta$. Then

$$D[p] * D[q] \subset \nu^{-1}(\alpha) * \nu^{-1}(\beta) \subset \nu^{-1}(\alpha\beta) \subset \nu^{-1}(\Omega).$$

By the last lemma there neighborhoods U and V of $D[p]$ and $D[q]$, respectively, such that $U * V \subset \nu^{-1}(\Omega)$. This implies $\nu(U)\nu(V) \subset \Omega$. Finally, we remark that, by Lemma 12, $\nu(U)$ and $\nu(V)$ are neighborhoods of α and β .

The continuity of inversion is proved in the same manner, which completes the proof of the theorem.

6 Two subgroups

$\text{Gal}_L(T)$ has two canonical normal subgroups:

- $\Gamma_1(T)$, the closure of $\{1\}$.
- $\text{Gal}_L^0(T)$, the connected component of 1.

Since $\text{Gal}_L(T)$ is quasicompact, we have

Lemma 19

1. *The quotient $\text{Gal}_L^\varepsilon(T) = \text{Gal}_L(T)/\Gamma_1(T)$ is a compact group, the closed Galois group of T .*
2. *$\text{Gal}_L^0(T)$ is the intersection of all closed (normal) subgroups of finite index.*

PROOF: $\text{Gal}_{\mathbb{L}}^c(T)$ is quasicompact and hausdorff, i.e. compact. For the second part, note that the quotient $\text{Gal}_{\mathbb{L}}(T)/\text{Gal}_{\mathbb{L}}^0(T)$ is totally disconnected ([12, §2]) and compact, whence a profinite group. In a profinite group the intersection of all normal closed subgroups of finite index is the identity. \square

An *imaginary* element of \mathbb{C} is a class of a \emptyset -definable equivalence relation on a cartesian power \mathbb{C}^n . Automorphisms of \mathbb{C} act in a natural way on imaginaries. An imaginary with only finitely many conjugates under $\text{Aut}(\mathbb{C})$ is called *algebraic*.

Let us prove that algebraic imaginaries are fixed by Lascar strong automorphisms: Let a/E be an algebraic imaginary with k conjugates. This means that E partitions the set of all conjugates of a into k classes. It follows that the type of a contains a formula $\varphi(x)$ whose realization set meets exactly k equivalence classes. Let f fix the model M . Then $\varphi(M)$ meets the same classes as $\varphi(\mathbb{C})$, which implies that a/E contains an element b of M , which must also belong to $f(a)/E$. It follows that $a/E = f(a)/E$.

This result extends easily to *hyperimaginaries*. Hyperimaginaries are equivalence classes of type-definable equivalence relations E , which are defined by a set of formulas Φ without parameters:

$$E(a, b) \Leftrightarrow \mathbb{C} \models \Phi(a, b).$$

a and b are, possibly infinite, tuples of elements of \mathbb{C} , of length smaller than $|\mathbb{C}|$. A hyperimaginary is *bounded* if it has less than $|\mathbb{C}|$ conjugates.

Lemma 20 *Bounded hyperimaginaries are fixed by Lascar strong automorphisms.*

PROOF: Let a/E be a bounded hyperimaginary and E defined by $\Phi(x, y)$. Then $\Phi \subset \Theta_\pi$, where $\pi = \text{tp}(a)$, since otherwise some $\theta \in \Phi$ would have antichains in $\pi(\mathbb{C})$ of arbitrary length, contradicting the assumption that a/E is bounded. If f is Lascar strong, a and $f(a)$ have the same Lascar strong type. By Corollary 9, $E(a, f(a))$. \square

If, conversely, a hyperimaginary h is fixed by all Lascar strong automorphisms, $f(h)$ is determined by the class of f in $\text{Gal}_{\mathbb{L}}(T)$. Whence h has no more than $2^{|T|}$ -many conjugates and is bounded.

We conclude that $\text{Gal}_{\mathbb{L}}(T)$ acts on bounded hyperimaginaries in a well defined way.

Theorem 21

1. $\Gamma_1(T)$ is the set of all elements of $\text{Gal}_{\mathbb{L}}(T)$ which fix all bounded hyperimaginaries.

2. $\text{Gal}_L^0(T)$ is the set of all elements of $\text{Gal}_L(T)$ which fix all algebraic imaginaries.

PROOF:

1. Let a/E be a bounded hyperimaginary and $\Gamma \leq \text{Gal}_L(T)$ the stabilizer of a/E . The preimage of Γ in $S_M(N)$ is

$$\nu^{-1}(\Gamma) = \{\text{tp}(f(M)/N) \mid f \in \text{Aut}(\mathbb{C}), E(f(a), a)\}.$$

Choose M containing a , let $N = M$ and E be axiomatized by Φ . Then

$$\nu^{-1}(\Gamma) = \{p(x) \in S_M(N) \mid \Phi(x', a) \subset p(x)\},$$

where the variables x' are a subtuple of x , as a is a subtuple of (m_i) , the enumeration of M . Whence Γ is closed and we conclude $\Gamma_1(T) \subset \Gamma$. This shows that the elements of $\Gamma_1(T)$ fix all bounded imaginaries.

For the converse consider the inverse image G_1 of $\Gamma_1(T)$ in $\text{Aut}(\mathbb{C})$. For $|T|$ -tuples a, b let $E(a, b)$ denote the equivalence relation of being in the same G_1 -orbit. Since the index of G_1 is bounded by $2^{|T|}$, E has at most $2^{|T|}$ classes. Since $\Gamma_1(T)$ is closed, E is type-definable. To see this, write the closed set $\nu^{-1}(\Gamma_1(T))$ as $\{p(x) \in S_M(N) \mid \Psi(x) \subset p(x)\}$ for a set $\Psi(x)$ of $L(N)$ -formulas. Then

$$E(a, b) \Leftrightarrow \text{for some } f \in \text{Aut}(\mathbb{C}) \quad \mathbb{C} \models f(a) = b \wedge \Psi(f(M)).$$

This shows, by an argument similar to that in the proof of Lemma 17, that E can be defined by a set of formulas with parameters from M and N . Since $\Gamma_1(T)$ is a normal subgroup, G_1 is a normal subgroup of $\text{Aut}(\mathbb{C})$. This implies that E is invariant under automorphisms, and whence can be defined by a set of formulas without parameters.

Now assume that $\alpha \in \text{Gal}_L(T)$ fixes all bounded hyperimaginaries. Take a model K of cardinality $|T|$ and consider it as a $|T|$ -tuple. Then K/E is a bounded hyperimaginary and fixed by α . This means that α is represented by an automorphism which agrees on K with an automorphism f from G_1 . Since K is a model, this implies that α is represented by f and belongs to $\Gamma_1(T)$.

2. Let i be an algebraic imaginary and Γ the stabilizer of i in $\text{Gal}_L(T)$. Γ is closed and has finite index, since the index equals the number of conjugates of i . It follows that $\text{Gal}_L^0(T) \subset \Gamma$. Thus the elements of $\text{Gal}_L^0(T)$ fix all algebraic imaginaries.

For the converse it suffices to show that every normal closed $\Gamma \leq \text{Gal}_L(T)$ of finite index is the stabilizer of an algebraic imaginary. The first part of the proof shows that Γ , being a normal⁵ closed subgroup, is the stabilizer of a bounded

⁵A slight variation of the argument shows that normality is not necessary: Let G be the preimage of Γ , and K a model of size $|T|$. Define $E(a, b)$ to be true if $a = b$ or, for some $f \in \text{Aut}(\mathbb{C})$ and $g \in G$, $f(K) = a$ and $fg(K) = b$. Then K/E is a bounded hyperimaginary with Γ as its stabilizer. See [7, 4.12].

hyperimaginary a/E . Since Γ has finite index, a/E has only a finite number of conjugates. We will show that a/E has the same stabilizer as an algebraic imaginary a/F . (If a is an infinite tuple, we can replace it by the finite subtuple of elements which occur in F .)

Let E be defined by Φ and let $a_1/E, \dots, a_n/E$ be the different conjugates of a/E . By compactness there is a symmetric formula⁶ $\theta \in \Phi$ such that no pair (a_i, a_j) ($i \neq j$) satisfies $\theta^2 = \theta \circ \theta$.⁷ This means that the sets $\theta(a_i, \mathbb{C})$ are disjoint. Since they cover the set of conjugates of a , there is a formula $\varphi(x)$ satisfied by a such that the intersections

$$D_i = \varphi(\mathbb{C}) \cap \theta(a_i, \mathbb{C})$$

form a partition of $\varphi(\mathbb{C})$. In order to ensure that this partition is invariant under automorphisms, we choose $\theta \in \Phi$ so small that no pair (a_i, a_j) satisfies θ^4 . This implies that $\theta^2(c, d)$ is never true for $c \in D_i$ and $d \in D_j$ and, therefore, that

$$F(x, y) = (\neg\varphi(x) \wedge \neg\varphi(y)) \vee (\varphi(x) \wedge \varphi(y) \wedge \theta^2(x, y))$$

defines an equivalence relation, with classes $\neg\varphi(\mathbb{C}), D_1, \dots, D_n$. Thus a/F is an algebraic imaginary. Since a/E and a/F contain the same conjugates of a , they have the same stabilizer. \square

Corollary 22

1. $\text{Gal}_{\mathbb{L}}^c(T)$ is the automorphism group of the set of all bounded hyperimaginaries of length $|T|$.
2. $\text{Gal}_{\mathbb{L}}(T)/\text{Gal}_{\mathbb{L}}^0(T)$ is the automorphism group of the set of all algebraic imaginaries.

\square

It was shown in [7] that every bounded hyperimaginary has the same (point-wise) stabilizer as a set of bounded hyperimaginaries of finite length. So $\text{Gal}_{\mathbb{L}}^c(T)$ is the automorphism group of the set of all bounded hyperimaginaries of finite length.

The set of algebraic imaginaries is often called $\text{acl}^{\text{eq}}(\emptyset)$. The group

$$\text{Gal}_{\mathbb{L}}(T)/\text{Gal}_{\mathbb{L}}^0(T) = \text{Aut}(\text{acl}^{\text{eq}}(\emptyset))$$

is the Galois group introduced by Poizat in [9].

For stable T two tuples a and b which have the same *strong* type (i.e. the same type over $\text{acl}^{\text{eq}}(\emptyset)$) have the same type over any model which is independent from ab . It follows that $\text{Gal}_{\mathbb{L}}^0(T) = 1$. This was extended to supersimple theories in [1]. Whether this is true for all simple⁸ theories is an open problem. All we know is Kim's result ([5]) that $\Gamma_1(T) = 1$ for simple T .

⁶Assume Φ closed under conjunction.

⁷Recall that $\theta(x, y)$ is the formula $\exists z \theta(x, z) \wedge \theta(z, y)$.

⁸See [11] for an introduction to simple theories.

7 Two Examples

The first part of this section is concerned with the proof of the following unpublished result of E. Bouscaren, D. Lascar and A. Pillay:

Theorem 23 *Any compact Lie group is the Galois group of a countable complete theory.*

First we need a lemma on O-minimal structures. Recall that a structure M with a distinguished linear order $<$ is O-minimal if every definable subset of M is a union of finitely many points and intervals with endpoints in M . Note that every structure elementarily equivalent to an O-minimal structure is itself O-minimal.

Lemma 24 *Every automorphism of a big saturated O-minimal structure is Lascar strong.*

PROOF: Let \mathbb{C} be a big saturated O-minimal structure. We prove that any two small submodels M, N of the same type have the same type over some model K . This implies, as in the proof of Lemma 1, that every automorphism which maps M to N is the product of an automorphism which fixes M and an automorphism which fixes K .

It is enough (and equivalent, see the proof of Lemma 7 (1)) to show the following : Every consistent formula $\varphi(z)$ has a realization c over which M and N have the same type.

We prove this by induction on the length of z . Assume that z consists of a tuple z_1 and a single variable z_2 . By induction there is a realization c_1 of $\exists z_2 \varphi(z_1, z_2)$ over which M and N have the same type. Let $\psi(m, c_1, z_2)$ be any formula over $M c_1$, and let the tuple $n \in N$ correspond to m . By O-minimality, and since m and n have the same type over c_1 , either both $\psi(m, c_1, \mathbb{C})$ and $\psi(n, c_1, \mathbb{C})$ contain a non-empty final segment of $\varphi(c_1, \mathbb{C})$ or $\neg\psi(m, c_1, \mathbb{C})$ and $\neg\psi(n, c_1, \mathbb{C})$ contain a non-empty segment. If we choose c_2 in the intersection of all these segments, $c = c_1 c_2$ realizes $\varphi(z)$ and M and N have the same type over c . \square

Now fix a compact Lie group G . The group G together with its structure of a real analytic manifold can be defined inside an expansion \mathcal{R} of the field \mathbb{R} by a finite number of analytic functions which are defined on bounded rectangles. By a result of van den Dries \mathcal{R} is O-minimal⁹ (see [10]).

Let \mathcal{R}^* a big saturated extension of \mathcal{R} and G^* the resulting extension of G . The intersection μ of all \emptyset -definable neighborhoods of the unit element of G^* is

⁹As A. Pillay has told me, compact Lie groups are semi-algebraic. This means that here (and in the proof of Corollary 26) one can actually assume that \mathcal{R} is the field of reals with a finite tuple of named parameters.

the normal subgroup of *infinitesimal* elements. The compactness of G implies that every element of G^* differs by an infinitesimal from some element of G . Whence G^* is the semi-direct product of G and μ .

Lemma 25 μ is the set of all commutators $[\varphi, h] = h^{-1}\varphi(h)$, where $h \in G^*$ and $\varphi \in \text{Aut}(\mathcal{R}^*)$.

PROOF: Let φ be an automorphism of \mathcal{R}^* and let h differ from $h_0 \in G$ by an infinitesimal ε . Since φ fixes \mathbb{R} , it fixes h_0 . Whence $h^{-1}\varphi(h) = (h_0\varepsilon)^{-1}\varphi(h_0\varepsilon) = \varepsilon^{-1}\varphi(\varepsilon)$ is infinitesimal.

Let conversely $\varepsilon \in \mu$ be given. Consider a *generic* type $p \in S(\emptyset)$ of G (cf. [8]). This means that p can be axiomatized by formulas which define (non-empty) open subsets $O(G)$ of G . Each $O(G^*)$ contains two elements h and $h\varepsilon$ (pick any $h \in O(G)$). Whence, by saturation, p has two realizations h and $h\varepsilon$. Choose an automorphism φ with $\varphi(h) = h\varepsilon$. Then $\varepsilon = h^{-1}\varphi(h)$.¹⁰ \square

Consider the two-sorted structure

$$\mathcal{M} = (\mathcal{R}, X, \cdot)$$

where \cdot is a regular action of G on the set X . We will show that G is the Galois group of the complete theory of \mathcal{M} .

Let $\mathcal{M}^* = (\mathcal{R}^*, X^*)$ be a big saturated elementary extension of \mathcal{M} . To describe the automorphisms of \mathcal{M}^* we fix a base point $x_0 \in X^*$. Any element of X^* can then uniquely be written as

$$x = h \cdot x_0$$

for some $h \in G^*$. We extend each automorphism φ of \mathcal{R}^* to \mathcal{M}^* by

$$\bar{\varphi}(x) = \varphi(h) \cdot x_0.$$

The automorphisms which leave \mathcal{R}^* fixed have the form \bar{g} , where

$$\bar{g}(x) = hg^{-1} \cdot x_0.$$

This implies that every automorphism of \mathcal{M}^* is a product

$$\Phi = \bar{g}\bar{\varphi}.$$

Note the commutation rule $\bar{\varphi}\bar{g} = \overline{\varphi(g)}\bar{\varphi}$.

Elementary substructures of \mathcal{M}^* have the form $(\mathcal{R}', G' \cdot x)$, where \mathcal{R}' is an elementary substructure of \mathcal{R}^* and $x = h \cdot x_0$ is any element of X^* . Therefore an automorphism fixes a submodel iff it can be written as $\bar{h}^{-1}\bar{\varphi}\bar{h}$, for some φ

¹⁰A variant of the proof shows that one can find a φ which fixes an elementary submodel of \mathcal{R}^* .

which fixes an elementary submodel of \mathcal{R}^* . It follows that an automorphism is Lascar strong iff it is a product of conjugates of automorphisms of the form $\bar{\varphi}$, for Lascar strong φ .

By Lemma 24 all φ are Lascar strong. The formula

$$\bar{h}^{-1}\bar{\varphi}\bar{h} = \overline{[\varphi, h]}\bar{\varphi},$$

together with the last Lemma, implies that $\Phi = \bar{g}\bar{\varphi}$ is Lascar strong iff g is infinitesimal. We conclude that

$$g \mapsto \text{class of } \bar{g}$$

defines an isomorphism $\iota : G \rightarrow \text{Gal}_{\mathbb{L}}(\mathcal{M}^*)$.¹¹

Finally we have to prove that ι is a homeomorphism. Let $U(G)$ be a \emptyset -definable neighborhood of $1 \in G$. Consider the map $\nu : S_{\mathcal{M}}(\mathcal{M}) \rightarrow \text{Gal}_{\mathbb{L}}(\mathcal{M}^*)$. Then $\nu^{-1}\iota(U(G))$ consists of those $\text{tp}(f(\mathcal{M})/\mathcal{M})$ for which $\mathcal{M}^* \models U(f(1))$. Whence, if 1 has index 1 in the enumeration of \mathcal{M} ,

$$\nu^{-1}\iota(U(G)) = \{p \in S_{\mathcal{M}}(\mathcal{M}) \mid U(x_1) \in p\}.$$

This proves that $\iota(U_n)$ is open. So ι is an open map. Since $\text{Gal}_{\mathbb{L}}(\mathcal{M}^*)$ is quasicompact and G is hausdorff, ε must also be continuous. *This completes the proof of Theorem 23.*

Corollary 26 *Every compact group is the Galois group of a complete theory.*

PROOF: Let G be a compact group. G is the direct limit of a directed system $(G_i, f_{i,j})_{i \leq j \in I}$ of compact Lie groups ([12, §25]). Again let \mathcal{R} be an expansion of the reals by bounded analytic functions, in which all the G_i and the maps f_{ij} can be defined. The elements of G are then given by certain infinite tuples $g = (g_i)_{i \in I}$ from the direct product of the G_i .

G will be the Galois group (of the complete theory) of the many-sorted structure

$$\mathcal{M} = (\mathcal{R}, X_i, f'_{ij})_{i \leq j \in I},$$

where the directed system of sets $(X_i, f'_{i,j})_{i \leq j \in I}$ is a copy of $(G_i, f_{i,j})_{i \leq j \in I}$ and each G_i operates (regularly) on X_i as it operates on itself by left multiplication.

Let again \mathcal{M}^* be a big saturated elementary extension of \mathcal{M} and G^* the inverse limit of the G_i^* . We call an element $\varepsilon = (\varepsilon_i)$ of G^* infinitesimal if all its components are infinitesimal. Let μ the subgroup of all infinitesimals. It is easy to see that G is isomorphic to the quotient G^*/μ .

Fix a base point $x_0 = (x_{0i})_{i \in I}$ in the (non-empty) inverse limit of the X_i^* . Then every automorphism of \mathcal{M}^* has the form $\Phi = \bar{g}\bar{\varphi}$ for $\varphi \in \text{Aut}(\mathcal{R}^*)$ and

¹¹The proof shows that two elements of X^* differ by an infinitesimal if they have the same Lascar strong type. It is easy to verify that this happens iff they have the same type over a submodel of \mathcal{M}^* .

$g \in G^*$, where \bar{g} and $\bar{\varphi}$ are defined as in the proof of the theorem. Thus, it suffices to show that Φ is Lascar strong iff g is infinitesimal.

Assume first that Φ is Lascar strong. Then each g_i is infinitesimal, since Φ restricted to (\mathcal{R}^*, X_i) is Lascar strong. Conversely, if g is infinitesimal, we find for every i an $h_i \in G_i$ such that h_i and $h_i g_i$ have the same type. A compactness argument shows that we can find the sequence (h_i) in G^* . Then h and hg have the same type. Let ψ be an automorphism of \mathcal{R}^* with $\psi(h) = hg$. As in the proof of the theorem, it is easy to see that $\bar{g}\bar{\psi} = \bar{h}^{-1}\bar{\psi}\bar{h}$ is Lascar strong. Whence also $\Phi = (\bar{h}^{-1}\bar{\psi}\bar{h})\psi^{-1}\bar{\varphi}$ is Lascar strong. \square

We construct our second example from the circle group S , the unit circle in the complex number plane. Let us fix some notation: λ_s denotes multiplication by s . R is the cyclic ordering on S , where $R(r, s, t)$ holds if s comes before t in the counter-clockwise ordering of $S \setminus \{r\}$.

Fix a natural number N , write σ_N for $\lambda_{\frac{2\pi i}{N}}$ and consider the structure

$$\mathcal{S}_N = (S, R, \sigma_N).$$

Let \mathbb{C}_N a big saturated elementary extension and f an automorphism of \mathbb{C}_N . If f is Lascar strong, let $|f|$ be the smallest n such that f is the product of n automorphisms which fix elementary submodels. If f is not Lascar strong, write $|f| = \infty$.

We will make use of the following lemma, which can be proved from Lemma 24 (see [2] for details).

Lemma 27

1. Every automorphism of \mathbb{C}_N is the product of some σ_N^n and some f with $|f| \leq 2$.
2. $|\sigma_N^n| = |n| + 2$, whenever $0 < |n| \leq \frac{N}{2}$.

Let \mathcal{S}_∞ be the disjoint union of the $\mathcal{S}_1, \mathcal{S}_2, \dots$ viewed as a many-sorted structure¹² with saturated extension $\mathbb{C}_\infty = (\mathbb{C}_1, \mathbb{C}_2, \dots)$.

Theorem 28 ([2]) *For each N let C_N be the N -element cyclic group with generator c_N . Let B be the group of all sequences $(c_N^{e_N})$ with a bounded sequence (e_N) of exponents. Then*

$$\text{Gal}_L(\mathbb{C}_\infty) \cong \prod_N C_N/B.$$

$\text{Gal}_L(\mathbb{C}_\infty)$ carries the indiscrete topology.

¹²We take also the disjoint union of the languages.

PROOF: The map $(c_N^{e_N}) \mapsto (\sigma_N^{e_N})$ defines a map from $\prod_N C_N$ to $\text{Aut}(\mathbb{C}_\infty)$, which yields a homomorphism

$$\mu : \prod_N C_N \rightarrow \text{Gal}_L(\mathbb{C}_\infty).$$

Let (f_N) be any automorphism of \mathbb{C}_∞ . If we apply part 1 of the Lemma to each component we see that we can write (f_N) as a product of some $(\sigma_N^{e_N})$ and two automorphisms which fix a model. This shows that μ is surjective.

Let $(c_N^{e_N})$ be an arbitrary element of $\prod_N C_N$. We can assume that $|e_N| \leq \frac{N}{2}$. Then by part 2 of the lemma it is immediate that $(\sigma_N^{e_N})$ is Lascar strong iff (e_N) is bounded, which means that B is the kernel of μ .

It remains to show that the topology of $\text{Gal}_L(\mathbb{C}_\infty)$ is indiscrete, or

$$\text{Gal}_L(\mathbb{C}_\infty) = \Gamma_1(\mathbb{C}_\infty).$$

The preimage of $\Gamma_1(\mathbb{C}_\infty)$ in $\text{Aut}(\mathbb{C}_\infty)$ is, by the next Lemma, a closed subgroup, which contains $\text{Aut}_L(\mathbb{C}_\infty)$. The automorphisms which fix almost every C_N are Lascar strong and form a dense subset of $\text{Aut}(\mathbb{C}_\infty)$. Thus the preimage of $\Gamma_1(\mathbb{C}_\infty)$ is the whole $\text{Aut}(\mathbb{C}_\infty)$ group. \square

We conclude with a general lemma. Let M be a model of T and consider the topology of *point-wise convergence* on $\text{Aut}(M)$, with basic open sets

$$U_{a,b} = \{f \mid f(a) = b\},$$

where a, b are finite tuples from M .

Lemma 29 *The natural map $\text{Aut}(M) \rightarrow \text{Gal}_L(T)$ is continuous.*

PROOF: Let Ω be a neighborhood of the image of f in $\text{Gal}_L(T)$. The preimage of Ω under¹³ $\nu : S_M(N) \rightarrow \text{Gal}_L(T)$ contains a basic neighborhood

$$O = \{p \mid \varphi(x) \in p\}$$

of $\text{tp}(f(M)/N)$. Let a be the tuple of elements of M which are enumerated by the free variables of φ . Then

$$O = \{\text{tp}(g(M)/N) \mid \mathbb{C} \models \varphi(g(a))\} \subset \{\text{tp}(g(M)/N) \mid g(a) = f(a)\}.$$

Whence $U_{a,f(a)}$ is a neighborhood of f which is mapped into Ω . \square

¹³ N can be any small model.

References

- [1] Steve Buechler, Anand Pillay, and Frank O. Wagner. Supersimple theories. *J. Amer. Math. Soc.*, 14:109–124, 2001.
- [2] E. Casanovas, D. Lascar, A. Pillay, and M. Ziegler. Galois groups of first order theories. 19 pages, submitted, 2000.
- [3] Wilfried Hodges. *Model Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1993.
- [4] Ehud Hrushovski. Simplicity and the lascar group. Preprint, 1997.
- [5] Byunghan Kim. A note on lascar strong types in simple theories. *J. Symbolic Logic*, 63:926–936, 1998.
- [6] Daniel Lascar. The category of models of a complete theory. *J. Symbolic Logic*, 47:249–266, 1982.
- [7] Daniel Lascar and Anand Pillay. Hyperimaginaries and automorphism groups. *J. Symbolic Logic*, 66(1):127–143, 2001.
- [8] Anand Pillay. On groups and fields definable in o-minimal structures. *J. Pure Appl. Algebra*, 53:239–255, 1988.
- [9] Bruno Poizat. Une théorie de galois imaginaire. *J. Symbolic Logic*, 48(4):1151–1170, December 1983.
- [10] Lou van den Dries. A generalization of the Tarski–Seidenberg Theorem and some non-definability results. *Bull. Amer. Math. Soc. (N.S.)*, 15(2):189–193, October 1986.
- [11] Frank O. Wagner. *Simple Theories*, volume 503 of *Mathematics and Its Applications*. Kluwer Academic Publishers, Dordrecht, NL, 2000.
- [12] André Weil. *L'intégration dans les groupes topologiques*. Actualités scientifiques et industrielles. Hermann, Paris, 2. edition, 1951.