M4 and M5 extra material for P11 Galois theory, Oct–Dec 2015.

Kevin Buzzard

1 Introduction / overview / waffle.

The goal of the Mastery/Comprehension element of the Galois theory course is to understand how to generalise the Fundamental Theorem of Galois Theory so that it applies to infinite extensions too. A (perhaps rather terse) reference is section 1 of "Profinite Groups" by K. Gruenberg, which can be found as chapter 5 of "Algebraic Number Theory" by Cassels and Froehlich.

Here is the theorem. Recall that an extension L/K of fields is *Galois* if it is algebraic, normal and separable. This is genuinely more general than being just finite normal and separable – for example if $K = \mathbf{Q}$ and $L = \overline{\mathbf{Q}}$, the set of all algebraic numbers in $\mathbf{C}$, then L/K is infinite, algebraic, normal (clear if you think about it) and separable (because we're in characteristic zero). This means that $\overline{\mathbf{Q}}/\mathbf{Q}$ is a Galois extension.

The Galois group $\mathrm{Gal}(L/K)$ of a Galois extension of fields is exactly what you think it is – it is just the field automorphisms of L which are the identity on K.

If $[L : K] = \infty$ then the size of $G := \mathrm{Gal}(L/K)$ will be infinite too; this will need proof, but it's true, and a good start.

However then things go a bit wrong – in general it is *not* true that there's a natural bijection between the intermediate field extensions $K \subseteq E \subseteq L$ and the subgroups of G. But there is a *really* neat fix! The idea is that G carries a very natural topology on it, and everything in sight is continuous, and the theorem is that intermediate field extensions correspond (in a natural bijective way) to *closed* subgroups of G, and the dictionary is just the same: to the field E we associate the subgroup $\{h \in G \mid h(e) = e \,\forall\, e \in E\}$ and this is the bijection.

All the other statements of the fundamental theorem generalise in the obvious way (normal extensions correspond to normal subgroups, and so on). If you regard a finite Galois group, of the kind we thought about in lectures, as having the discrete topology, then every subset is open and closed, and in particular every subgroup is closed, so the usual fundamental theorem can also be thought of as a bijection between intermediate fields and closed subgroups. However in the infinite case there will usually be subgroups that aren't closed, and they don't correspond to any subfields.

One piece of good news – a proof of the fundamental theorem in the infinite case can be *deduced* from the assertion in the finite case, so we don't have to re-do all the intermediate lemmas and so on – in fact the main work we have to do is to explain how we put a topology on $\mathrm{Gal}(L/K)$. This topology is not like the kinds of topologies you usually see in an introductory course – it has a rather different flavour to the usual topology on $\mathbf{R}^n$. For example the topology on a Galois group is *totally disconnected*, which means that the only connected subsets are subsets with one element. The topology on an infinite Galois group is very much like the topology on the p-adic numbers – you may have seen these things in, for example, the elliptic curves course. Indeed there is an infinite extension of fields whose Galois group is isomorphic to the p-adic integers.

This was new material for 2014-15 so all you have in the way of past papers or questions is last year's Mastery exam (the system was different last year). So this note may look a little long, but that's not because it's complicated or full of hard material – it's long because I will explain everything slowly and carefully. If you want to know how to prepare for the mastery exam – make sure you understand well the construction of the topology on an infinite Galois group, and make sure you know the statement of the fundamental theorem of Galois theory for an infinite Galois field extension, because that is what I am trying to teach you.

2 Topological groups.

A *topological group* is a group G such that the underlying set G has the structure of a topological space, in such a way that multiplication $G \times G \to G$ and inversion $G \to G$ (the map sending g to

g^{-1}) are continuous (put the product topology on $G \times G$, which means that a basis for the open sets are things of the form $U \times V$ with U and V open in G). Examples of topological groups are everywhere – indeed most if not all groups you have seen that have natural topologies on them (for example the real numbers under addition) will be topological groups. Fields such as as $\mathbf{R}$, $\mathbf{C}$, the p-adic numbers $\mathbf{Q}_p$ (if you know what they are) are all topological groups under addition. You can build plenty more topological groups from them too, such as $\mathrm{GL}_n(\mathbf{R})$, $\mathrm{GL}_n(\mathbf{C})$, or slightly more exotic groups like $O_n(\mathbf{R})$ (the orthogonal groups), or $\mathrm{Sp}_{2n}(\mathbf{R})$ (the symplectic groups) if you know what these things are. It doesn't matter if you don't though – such groups are not the kinds of groups that show up as infinite Galois groups.

Let me explain an example of a topological group which is much more like the kind of group that shows up. Before I do that I need to explain how to do infinite products of topological spaces.

2.1 Infinite products of topological spaces.

If I is a set (probably infinite), and for each $i \in I$ we have a topological space X_i, then I want to define a topological space $X = \prod_i X_i$. As a set, X is just what you think it is: an element of X is just an element from each X_i, so it's a collection $(x_i)_{i \in I}$, with $x_i \in X_i$ for all $i \in I$. The interesting thing is the topology. If you've seen the definition of a finite product of topological spaces, you would know exactly what to guess – we could take $U_i \subseteq X_i$ an open set, for all i, and then say that $\prod_i U_i \subseteq \prod_i X_i$ is open and furthermore that these form a basis of open sets for the product topology. This looks like a nice idea but it is unfortunately *not* the right idea. The reason is that we want to make sure that the topology on X is somehow "the weakest topology such that the natural projection maps $X \to X_i$ are all continuous" (i.e. the topology with the fewest open sets that makes all the maps continuous), and thinking about this (see the first question on the example sheet) leads us to the following definition:

Definition. The topology on $\prod_i X_i$ is defined as follows. Choose open sets $U_i \subseteq X_i$ for all i, but with the extra condition that $U_i = X_i$ for all but finitely many i. A basis for the topology on $\prod_i X_i$ are the sets $\prod_i U_i$ of this form. As usual, a set if open if and only if it is a union of elements of this basis.

As I say, the first exercise on the example sheet indicates why this is the right topology.

2.2 Infinite products of finite groups.

Let I be a set and for $i \in I$, let G_i be a finite group. Regard each G_i as a topological space with the discrete topology – recall that this is the silly topology where every subset of G_i is open. Define $G = \prod_i G_i$, and put the product topology on G. It is easy to check that G is a group – the group law is just defined pointwise, the identity is the element which is the identity on each component, and each of the group axioms hold for G because their truth is inherited from the corresponding axiom for each G_i. We also know that G is a topological space – give it the product topology. The G_i's all had the discrete topology, but it is *not* true in general that G will have the discrete topology! See Q3 on the example sheet. A point in the product will be closed, but not open in general. Anyway, that's not what we need to worry about right now – what we need to worry about right now is whether G with its product topology becomes a topological group – in other words, whether the topology and the group law play well together. Indeed, they do.

Lemma 2.1. *G with its product topology becomes a topological group.*

Proof. We need to check that multiplication $G \times G \to G$ and the inverse map $G \to G$ are continuous. Let's do this.

Let's start with multiplication. It suffices to check that the pre-image of a basic open set $U = \prod_i U_i \subseteq G$ is open in $G \times G$. Say I_0 is a finite subset of I such that $U_i = G_i$ for all $i \notin I_0$; such a finite set I_0 exists by the definition of a basic open set. Say $(g, h) \in G \times G$ is in the pre-image of U; this is just a silly way of saying that $gh \in U$. Let's write $g = (g_i)$ and $h = (h_i)$. Let's check that there are basic open sets V and W in G such that $g \in V$, $h \in W$, and such that for all $v \in V$ and $w \in W$, we have $vw \in U$. This will suffice, because then $V \times W$ is in the pre-image of U. In

fact such sets V and W are very easy to define: set $V_i = \{g_i\}$ if $i \in I_0$ and $V_i = G_i$ otherwise; similarly set $W_i = \{h_i\}$ if $i \in I_0$ and $W_i = G_i$ otherwise. It's very easy to check that $V = \prod_i V_i$ and $W = \prod_i W_i$ have the properties we require (note that $gh \in U$ and hence $g_i h_i \in U_i$ for all i).

Next let's do inversion; this is just as easy, because if $U = \prod_i U_i$ is a basic open set then $U_i = G_i$ for all but finitely many i, and if $V_i = U_i^{-1} = \{u_i^{-1} : u_i \in U_i\}$ then $V_i = G_i$ for all but finitely many i, and $V = \prod_i V_i$ is basic open and the pre-image of U under the inversion map. □

2.3 Projective limits of finite groups.

Now we let I be not just a set, but a *directed set*. This means that I is equipped with a relation $\leq$ (recall: a *relation* $\leq$ on a set I is, formally speaking, a subset of $I \times I$, and informally it's just, for every pair of elements i, j a way of deciding whether $i \leq j$ or not) and this relation had better satisfy some axioms, which I'm about to tell you. Firstly, it has to satisfy the axioms for a *partial order*:

(i) [Reflexivity] $i \leq i$ for all $i \in I$;

(ii) [Transitivity] If $i \leq j$ and $j \leq k$ then $i \leq k$;

(iii) [Antisymmetry] If $i \leq j$ and $j \leq i$ then $i = j$.

Important note: We do *not* demand that for all i and j, either $i \leq j$ or $j \leq i$; it might be the case that neither of these things hold. A good model to keep hold of is that I can be the set of subsets of a set S, and $i \leq j$ iff $i \subseteq j$; if S has size 2 or more then there will be subsets i and j with $i \not\subseteq j$ and $j \not\subseteq i$.

This is not quite the definition of a directed set: we also require a fourth axiom:

(iv) For all $i, j \in I$ there is $k \in I$ with $i \leq k$ and $j \leq k$.

Again, an example would be the set of subsets of a set; we could just take k to be the union of i and j for axiom (iv).

Another example: I could be $\mathbf{Z}$ or $\mathbf{Z}_{\geq 1}$ or $\mathbf{R}$ with the usual ordering.

Now here's the set-up. Say I is a directed set, and say for each $i \in I$ we have a finite group G_i. Furthermore, suppose that whenever $i \leq j$ we have a map $\pi_{j,i} : G_j \to G_i$, satisfying the following axioms:

(a) $\pi_{i,i}$ is the identity map for all i

(b) If $i \leq j \leq k$ then $\pi_{k,i} = \pi_{j,i} \circ \pi_{k,j}$ (note that $i \leq k$ by transitivity, so $\pi_{k,i}$ makes sense).

Here's an example: Let p be a prime, set $I = \{1, 2, 3, \ldots\}$, set $G_i = (\mathbf{Z}/p^i\mathbf{Z})$ and for $i \leq j$ let $\pi_{j,i}$ be the obvious projection map $\mathbf{Z}/p^j\mathbf{Z} \to \mathbf{Z}/p^i\mathbf{Z}$. The axioms are readily checked.

We define the *projective limit*, or the *inverse limit*, or sometimes just the *limit* of this inverse system of groups, to be the following topological group: it is the subspace Γ of the product $\prod_i G_i$ consisting of elements (g_i) such that $\pi_{j,i}(g_j) = g_i$ for all i.

Lemma 2.2. *The inverse limit Γ (equipped with the subspace topology) is a topological group.*

Proof. Let us first check that Γ is a group. We know that $G = \prod_i G_i$ is a group, and Γ is a subset of G. To check it's a subgroup we need to check that the identity is in (which is obvious, as $\pi_{j,i}(e_j) = e_i$ as all the $\pi_{j,i}$ are group homomorphisms), that if (g_i) is in then so is (g_i^{-1}) (which is clear, because if $\pi_{j,i}(g_j) = g_i$ then $\pi_{j,i}(g_j^{-1}) = g_i^{-1}$) and that if (g_i) and (h_i) are in then so is $(g_i h_i)$ (which is also clear, because if $\pi_{j,i}(g_j) = g_i$ then and $\pi_{j,i}(h_j) = h_i$ then $\pi_{j,i}(g_j h_j) = g_i h_i$).

Next we need to check that multiplication and inverse are continuous. But in fact these things are obvious, because they are true for G as we already checked, and Γ has the subspace topology so it inherits all the continuity statements we want. Alternatively just bash it all out. □

Notation: $\Gamma = \mathrm{proj}\lim_i(G_i)$ or $\Gamma = \varprojlim_i(G_i)$.

Example: if $I = \{1, 2, 3, \ldots\}$ and $G_i = \mathbf{Z}/p^i\mathbf{Z}$ then $\mathrm{proj}\lim_i G_i = \mathbf{Z}_p$, the p-adic integers (if you know what they are; if you don't then it's still true but is probably less helpful, unless you just learnt what they are from this, in which case it's helpful but not in the way I meant it to be).

Example: if I is anything and we define $i \leq j$ iff $i = j$, and set each $\pi_{j,i}$ to be the identity map, then $\mathrm{proj}\lim_i(G_i) = \prod_i G_i$.

Lemma 2.3. *If* $\Gamma = \operatorname{proj\,lim}_i G_i$ *with* G_i *finite, then* Γ *is a* closed *subset of* $G = \prod_i G_i$.

Proof. This is easy. Say $x = (x_i) \notin \Gamma$. Then by definition there exists j and k with $j \leq k$ and $\pi_{k,j}(x_k) \neq x_j$. Set $U_i = G_i$ unless $i = j$ or $i = k$; set $U_j = \{x_j\}$ and $U_k = \{x_k\}$. Set $U = \prod_i U_i$; then U is an open set containing x and furthermore $U \cap \Gamma$ is empty, because if $(u_i) \in U$ then $\pi_{k,j}(u_k) = \pi_{k,j}(x_k) \neq x_j = u_j$. □

Remark 2.3.1. Tychonoff's theorem says that a product of compact topological spaces is compact. In particular a product of finite topological spaces is compact. Moreover it's well-known that a closed subspace of a compact topological space is compact, and we conclude from the previous lemma that a projective limit of finite groups is compact. The proof of Tychonoff's theorem does use the Axiom of Choice (in an essential manner), but given that we're all consenting adults now, this should hopefully not bother you.

3 Infinite Galois groups.

Say L/K is an algebraic normal and separable extension. I am now going to show how $\mathrm{Gal}(L/K)$, the group of field isomorphisms $L \to L$ which are the identity on K, is naturally a group with a topology; I'm going to do this by identifying it with a projective limit of finite groups as in the previous section.

Say $\lambda \in L$. Then by definition λ is algebraic over K, so let $p(x)$ be its min poly. By definition of normality, $p(x)$ splits completely in L; let K_λ denote the subfield of L generated over K by the roots of $p(x)$. Now K_λ is finite over K, and it's also a normal extension of K (because it's a splitting field) and a separable extension of K (because it's a subfield of a separable extension). This means K_λ/K is a finite Galois extension, and hence has a Galois group $\mathrm{Gal}(K_\lambda/K)$.

Now let I be the set of all finite Galois extensions M/K with $K \subseteq M \subseteq L$. If M_1, $M_2 \in I$ then define $M_1 \leq M_2$ iff $M_1 \subseteq M_2$. By Problem sheet 6 Q6(ii) I is a directed set. For $M \in I$ write $G_M = \mathrm{Gal}(M/K)$; if $M_1 \leq M_2$ then the natural restriction map is a map $G_{M_2} \to G_{M_1}$ and one checks easily that the G_M form a projective system of finite groups. Let Γ denote their projective limit. Then Γ is a topological group, and it's compact if you believe Tychonoff's theorem.

Lemma 3.1. $\Gamma = \mathrm{Gal}(L/K)$.

Proof. If $f : L \to L$ is a field automorphism and f is the identity on K, then for each $M \in I$ the restriction of f to M is a map $M \to L$, and by problem sheet 4 Q7 the image of this map lands in M. The induced map $M \to M$ is a bijection (because it's a field map so it's an injection, and an injective linear map from a finite-dimensional vector space to itself is a bijection), and hence f gives us an element in $\mathrm{Gal}(M/K)$. In particular f gives us an element of $\prod_M \mathrm{Gal}(M/K)$, and it's clearly compatible with the restriction maps so it gives us an element of Γ. We get a map $\mathrm{Gal}(L/K) \to \Gamma$ which is easily checked to be a group homomorphism. It is injective because if two $f's$ agree on every $M \in I$ then (set $M = M_\lambda$) they agree on each $\lambda \in L$ and hence they agree (in other words, they agree because L is the union of the M's in I). It is surjective because given $\gamma = (g_M) \in \Gamma$ we can define $f : L \to L$ by $f(\lambda) = g_{M_\lambda}(\lambda)$; equivalently we can define $f(\lambda) = g_M(\lambda)$ for *any* $M \in I$ containing λ; this is well-defined because $(g_M) \in \Gamma$ so the g_M all agree on overlaps. □

Corollary 3.2. $\mathrm{Gal}(L/K)$ *inherits a natural topology (coming from* Γ*).*

4 The fundamental theorem of Galois theory.

Say L/K is algebraic, normal and separable. Let $\Gamma = \mathrm{Gal}(L/K)$ denote the field automorphisms of L which are the identity on K. Give Γ the topology defined in the previous section.

Theorem 4.1 (Fundamental theorem of Galois theory)**.** *There is an order-reversing bijection between the closed subgroups of* Γ *and the subfields of* L *containing* K*. The dictionary is the same as in the finite case – if* Δ *is a closed subgroup of* Γ *then define* $M = \{\lambda \in L : g(\lambda) = \lambda \, \forall g \in \Delta\}$*, and conversely if* $K \subseteq M \subseteq L$ *then define* $\Delta = \{g \in \Gamma : g(m) = m \, \forall m \in M\}$*.*

If Δ *corresponds to* M *via this bijection then* L/M *is Galois and* $\mathrm{Gal}(L/M) = \Delta$ *(both sides are naturally subgroups of* $\mathrm{Gal}(L/K)$ *and the equality is taking place in this group).*

Finally, Δ *is normal iff* M/K *is normal, and in this case* M/K *is Galois and* $\mathrm{Gal}(M/K) = \Gamma/\Delta$*.*

The proof is not hard. A sketch is on the example sheet. Note: *the proof is not part of the assessed material!* My initial plan was to make it part of the assessed material, but when I saw how much stuff was involved in even stating the result, I decided that asking you to learn the proof too was just too much.

So in summary then, that's a pretty crazy fix to make the fundamental theorem work in the infinite case. And there really will be non-closed subgroups, in general, in an infinite Galois group, so all this stuff really did need to be done – the fundamental theorem really would not work without this new idea.

One of the objects I study as a research mathematician is the infinite Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and how representations of this group can come from all sorts of crazy places, like modular forms, and so the fundamental theorem is the sort of thing I am always using in my work.