GALOIS THEORY : LECTURE 6

LEO GOLDMAKHER

1. What does it mean to generate a field?

We'll start with what first seems to be a point about definition–what does it mean to consider the "field generated by a set S"? Here's an informal definition:

Definition (informal)**.** The *field (or ring or group or...) generated by set S* is the smallest field (or ring or group or...) containing S.

Will then asked if we need our definition to deal with operations somehow (i.e. is just specifying a set enough?). Let's look at a quick example that will hopefully show us why we should care about operations:

Example 1. What is the field generated by $S = \{1\}$?

Eli suggested that the field generated by S is $\mathbb{F}_2$ (the field of two elements), and Michael pointed out that under ordinary addition and multiplication the field generated by S could be $\mathbb{Q}$. How do we choose? We need to revisit our definition and make sure it accounts for operations.

Let's try again – this time we'll make sure we specify an "ambient field" (that is, some field that we are going to inherit our operations from):

Example 2. Let $S = \{\sqrt{2}\}$. What is the field generated by S over $\mathbb{Q}$?

Jonah answered the question: the field generated by S over $\mathbb{Q}$ is $\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$. It is easy to see that this is a ring. To see it is a field we need to check that we can divide elements. The trick is using the conjugate, e.g.

$$\frac{3+\sqrt{2}}{5-\sqrt{2}} = \frac{3+\sqrt{2}}{5-\sqrt{2}} \cdot \frac{5+\sqrt{2}}{5+\sqrt{2}} = \frac{(3+\sqrt{2})(5+\sqrt{2})}{23} \in \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}.$$

Notice that our process of generating a field involved taking a known field (in this case, $\mathbb{Q}$) and attaching some new "stuff" (here, $\sqrt{2}$) in order to create a bigger field. Actually, there's a little bit of subtlety to this process–we had some sense of what $\sqrt{2}$ *is* (in particular, we knew that $(\sqrt{2})^2 = 2$) and that helped us to figure out the shape of the field generated by S. To make this more clear, we'll look at one more example and this time we'll again attach new "stuff" to $\mathbb{Q}$ but we won't really have a sense of what this new "stuff" is.

Example 3. Let $S = \{\sqrt{\text{orange}}\}$. What is the field generated by S over $\mathbb{Q}$?

We weren't really able to figure this one out, mainly because we don't know what $\sqrt{\text{orange}}$ is or where it lives or how it interacts with $\mathbb{Q}$ (are there any rational relations between $\sqrt{\text{orange}}$ and $\mathbb{Q}$?). So, we need to know what bigger field we are operating in; that is, we need to know an ambient field of $\mathbb{Q}$ in which $\sqrt{\text{orange}}$ exists. This motivates the following formal definition:

Definition. Given fields K and L such that $L \supseteq K$ and given $S \subseteq L$, the *field generated by S over $K \subseteq L$* is denoted $K(S)$ and defined as

$$K(S) := \bigcap_{\substack{K \subseteq F \subseteq L \\ \text{s.t. } S \subseteq F}} F.$$

Date: February 19, 2018.

Based on notes by Sumun Iyer.

Note that $K(S)$ is the "smallest field" containing S, just as we wanted in our informal definition. It is not hard to check that $K(S)$ is indeed a field.

To return to Example 2 with our new formal definition, the field generated by $S = \{\sqrt{2}\}$ over $\mathbb{Q} \subseteq \mathbb{C}$ is

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}.$$

We read $\mathbb{Q}(\sqrt{2})$ as "$\mathbb{Q}$ adjoin $\sqrt{2}$." Note that in this particular case, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

2. SOLVING POLYNOMIALS OVER FIELDS

Let's return to the question we were discussing at the end of last lecture–how do we solve the equation $x^2 + 1 = 0$ over the field $\mathbb{F}_3$? Alex posed the following idea at the end of the last class: try to adjoin the complex number i to $\mathbb{F}_3$. Unfortunately, there is a problem with this approach. As Beatrix pointed out, $\mathbb{F}_3$ is not actually contained in $\mathbb{C}$. We can see this because $[1] + [1] + [1] = [0]$ in $\mathbb{F}_3$ but $1 + 1 + 1 \neq 0$ in $\mathbb{C}$.

Perhaps we can be more flexible however–maybe there is some isomorphic copy of $\mathbb{F}_3$ that lives in $\mathbb{C}$. What do we mean by an "isomorphic copy"? Well, consider for example the spaces $\mathbb{R}$ and $\mathbb{R}^2$. We would say there is an isomorphic copy of $\mathbb{R}$ in $\mathbb{R}^2$ (we can think of picking up $\mathbb{R}$ and placing it on the horizontal axis of $\mathbb{R}^2$) even though $\mathbb{R}$ is not technically a subset of $\mathbb{R}^2$. In mathematical terms, we have an isomorphism $\mathbb{R} \xrightarrow{\sim} \mathbb{R} \times \{0\}$ which sends $r \mapsto (r, 0)$.[1] More generally, an isomorphic copy of a field F inside some other field K is the image $\phi(F)$ under some injective homomorphism $\phi : F \hookrightarrow K$. Note that if such a ϕ exists, then $F \simeq \phi(F)$, which allows us to discuss F using the language of K.

Even with our more flexible idea, we are still stuck. As Alex pointed out, the same argument Beatrix used to show that $\mathbb{F}_3 \not\subseteq \mathbb{C}$ works to show that there is no isomorphic copy of $\mathbb{F}_3$ in $\mathbb{C}$.

Proposition 1. *$\mathbb{F}_3$ does not embed into $\mathbb{C}$.*

Proof. Suppose $\phi : \mathbb{F}_3 \to \mathbb{C}$ is a homomorphism; we claim ϕ cannot be injective. To see this, first observe that

$$\phi([0]) = \phi([0] + [0]) = \phi([0]) + \phi([0]),$$

whence $\phi([0]) = 0$. Now, using the same idea as earlier:

$$0 = \phi([0]) = \phi([1] + [1] + [1]) = \phi([1]) + \phi([1]) + \phi([1]) = 3\phi([1]).$$

It follows that $\phi([1]) = 0 = \phi(1)$, and so ϕ is not injective. $\square$

Thus, we cannot adjoin the number $i \in \mathbb{C}$ to the field $\mathbb{F}_3$, since the proposition above shows that we can't describe $\mathbb{F}_3$ using the language of complex numbers (and in particular, there's no good way to describe the interaction between i and $\mathbb{F}_3$). Notice that the heart of the proof above is the idea that $[1] + [1] + [1] = [0]$ in $\mathbb{F}_3$ but $1 + 1 + 1 \neq 0$ in $\mathbb{C}$. This idea motivates a useful definition:

Definition. The *characteristic* of a field K (denoted by char K) is the least positive $n \in \mathbb{N}$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If no such n exists, then we say that char $K = 0$.

Proposition 2. *If* char $K \neq$ char K'*, then K does not embed into K'.*

Proof. See problem set 4. $\square$

Remark. Note that Proposition 2 immediately implies that if $K \simeq K'$, then char K = char K'. The converse of this statement does **not** hold, however.

[1] Note that under the natural operations $+$ and $\times$, $\mathbb{R}^2$ isn't a field. Why not? Can you find operations which do make it into a field?

It turns out that the characteristic of a field is always either 0 or a prime. In practice, proofs of theorems about field theory often split into two cases: characteristic 0 and positive characteristic, employing two different approaches.

When we discussed generating a field from a given set of elements, we required two additional pieces of information: a small field and a large ambient field. But as we've seen, we don't need to require that the small field literally live inside the large one; an isomorphic copy will do. We formalize this in the following definition:

Definition. Given two fields K and L we say that L is a *field extension* of K if and only if K embeds into L.

There are two common notations for field extensions. The better one is $\begin{array}{c} L \\ | \\ K \end{array}$. Unfortunately, this is typographically challenging, so most people end up using the simpler notation L/K. This has one annoying drawback: it looks like a quotient of L by K. In principle this is unambiguous, since K is not an ideal of L (unless $L = K$); in practice, of course, this can be confusing. Just keep in mind that when you see the symbol A/B, if A and B are both fields, then this is a field extension, whereas if A is a group or a ring, then this is a quotient.

Remark. Intuitively, if L is a field extension of K, you should think of K as being a subfield of L.

Armed with this new notion, we now return to our original question–how can we solve $x^2 + 1 = 0$ in $\mathbb{F}_3$? The following theorem will resolve our question.

Theorem 3. *(Kronecker, 1882) Given $f \in K[t]$ a non-constant polynomial, where K is a field. Then there exists L/K in which f has a root.*

Proof. (The short, short version.) We may assume that f is irreducible over $K[t]$ (why?). Let $L = K[t]/(f)$.
Step 1. L is a field (since we're modding a ring out by a maximal ideal).
Step 2. L is a field extension of K.
Step 3. f has a root in L. □

We will unpack this proof in detail next time. For now, we consider a concrete example.

Example 4. Let us try to follow the above outline to determine a root of $x^2 + 1$ over $\mathbb{Q}$. Set

$$L := \mathbb{Q}[t]/(t^2 + 1).$$

By definition, $L = \{[f(t)] \ : \ f \in \mathbb{Q}[t]\}$, where

$$[f_1(t)] = [f_2(t)] \quad \iff \quad f_1(t) \equiv f_2(t) \pmod{t^2+1} \quad \iff \quad (t^2+1) \mid (f_1(t) - f_2(t)).$$

For instance, you should check that $[2t^3 - t^2 + 4t + 1] = [-t^2 + 2t + 1] = [2t + 2]$. (Daishiro noted that we can take a clever shortcut by substituting -1 for t^2; this gives the same result.) Working a bit harder, we can show that $L = \{[at + b] \ : \ a, b \in \mathbb{Q}\}$. Is L actually a field? It's easy to verify that it's a commutative ring. Thus it remains only to check that multiplicative inverses exist. For example, is $\frac{[1]}{[t+6]} \in L$? Yes! To see this, Michael observed that we can use our favorite old trick:

$$\frac{[1]}{[t+6]} \cdot \frac{[-t+6]}{[-t+6]} = \frac{[-t+6]}{[-t^2+36]} = \frac{[-t+6]}{[37]} = \left[-\frac{1}{37}t + \frac{6}{37}\right] \in L.$$