GALOIS THEORY: LECTURE 5

FEBRUARY 15, 2023

1. Key Points from Algebra

Definition. We define a **field** to be any set K endowed with two binary operations $+$ and $\times$ such that K is an abelian group under addition with additive identity 0, and $K \setminus \{0\}$ is an abelian group under multiplication with multiplicative identity 1. Additionally, we must have that multiplication distributes over addition, ie $a(b+c) = ab + ac$ for all $a, b, c \in K$ and finally that $1 \neq 0$.

Examples of fields include the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the three-elements field $\mathbb{F}_3$, which one will also see denoted $\mathbb{Z}_3$ or $\mathbb{Z}/3\mathbb{Z}$.

Here are some sets we often encounter that are not fields: $\mathbb{Z}$, $\mathbb{Q}[t]$, $\mathbb{Z}_6$, and $\mathbb{R}^2$. (Actually, as Jonathan pointed out, the last of these can be made into a field by defining addition as usual and defining multiplication via $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$. In other words, we're secretly treating $\mathbb{R}^2$ as though it were $\mathbb{C}$.)

Definition. A set R is a **ring** if it has all the field properties except $R \setminus \{0\}$ doesn't necessarily have to have multiplicative inverses. Note that we require $1 \in R$ in this class, but we don't require that multiplication in R be commutative.

Any field is a ring. Other examples include $\mathbb{Z}$, $\mathbb{Q}[t]$, and $\mathbb{Z}_6$. Note that $3\mathbb{Z}$ is not a ring for our purposes, because it doesn't have a multiplicative identity.

Definition. Given a ring R, a subset $S \subseteq R$ is called a **subring** if S is a ring under inherited $+$ and $\times$ from R and has the same additive and multiplicative identities as R.

For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$. The subset $\{0, 3\} \subseteq \mathbb{Z}_6$ is not a subring because 1 is the multiplicative identity in $\mathbb{Z}_6$, whereas 3 is the multiplicative identity in the subset.

Similarly, $3\mathbb{Z} \subseteq \mathbb{Z}$ is not a subring since it doesn't inherit the multiplicative identity. It's still a nice subset though, because $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{F}_3$. We call $3\mathbb{Z}$ an ideal subset of $\mathbb{Z}$.

Definition. Given a ring R, we say $I \subseteq R$ is an **ideal subset** (or simply, an 'ideal') iff $I \trianglelefteq R$ under addition and R/I is a ring. Recall that $R/I := \{[x] : x \in R\}$ where $[x] = x + I$.

For example, $Z_6 = \mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$ where $[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$ and each other element is defined similarly.

We want to define $+$ and $\times$ on R/I as $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$.

This may not always be well-defined, though. Here's a cautionary example. Consider $\mathbb{Q} \subseteq \mathbb{Q}[t]$. Note that $\mathbb{Q} \trianglelefteq \mathbb{Q}[t]$ as groups under addition.

Then $\mathbb{Q}[t]/\mathbb{Q} = \{[f] : f \in \mathbb{Q}[t]\}$, where $[f] = f + \mathbb{Q}$.

We define $[f] + [g] = [f + g]$ and $[f][g] = [f \cdot g]$.

Then we have $[t^2] \ni t^2 + 2$, whence $[t^2] = [t^2 + 2]$. It follows that $[t][t^2] = [t][t^2 + 2]$. But this means $[t^3] = [t^3 + 2t]$, which is a contradiction, since these differ by $2t$, and $2t \notin \mathbb{Q}$! Thus, $\mathbb{Q}$ is not an ideal of $\mathbb{Q}[t]$. Analyzing this more carefully leads to the following characterization of ideals:

Proposition 1. *$I \subseteq R$ is an ideal iff*

(1) $I \trianglelefteq R$ under $+$

(2) $RI \subseteq I$ and $IR \subseteq I$. ('I swallows multiplication.')

Here are some examples of ideals of $\mathbb{Q}[t]$:

Summary of a lecture by Leo Goldmakher; typed by Jacob Lehmann Duke from notes by Noah Cape. (Thanks, Noah!)

(1) Polynomials with $a_0 = 0$
(2) $\langle t+1 \rangle := (t+1)\mathbb{Q}[t]$, the set of all multiples of $(t+1)$. This ideal is said to be *generated* by $t+1$, meaning it's the minimal ideal containing $t+1$.
(3) Pick $\alpha \in R$. The set of all polynomials with α as a root forms an ideal of R.

Definition. Given a field K, we say $f \in K[t]$ is **irreducible** iff $f = gh$ with $g, h \in K[t]$ implies g or h is a unit. This is saying that f cannot be broken down in a meaningful way into smaller polynomials.

Definition. We say $\alpha \in R$ is a **unit** iff there exists $\alpha^{-1} \in R$ such that $\alpha\alpha^{-1} = 1$. We denote the set of all units of R by $R^\times$. Note that in a field, all nonzero elements are units, so if K is a field, then $K^\times = K \setminus \{0\}$.

For more on rings, check out the document posted on the course website!