GALOIS THEORY : LECTURE 5

LEO GOLDMAKHER

1. Some Preliminary Investigation of Polynomial Rings

We opened with a question:

Question 1. *What does it mean for a polynomial $f \in \mathbb{Q}[x]$ to be irreducible?*

Will took a first stab at answering this: a polynomial $f \in \mathbb{Q}[x]$ is irreducible if it cannot be factored into two components, $f = gh$, where $g, h \in \mathbb{Q}[x]$. However, Beatrix pointed out this does not quite capture what it means to be irreducible, since we can write *any* $f \in \mathbb{Q}[x]$ as the product of two other polynomials. For example,

$$x^2 + 4x + 6 = (1) \cdot (x^2 + 4x + 6),$$

or slightly less trivially,

$$x^2 + 4x + 6 = (1/2) \cdot (2x^2 + 8x + 12).$$

In view of these examples, we state a formal definition.

Definition. Given a field K, $f \in K[t]$ is *irreducible* iff $f = gh$ for $g, h \in K[t]$ implies $g \in K$ or $h \in K$.

This is highly reminiscent of factorization in the integers, where a prime can only be factored as a product of 1 and itself. The case of irreducible polynomials is like this, but with more 'units' in addition to 1. This inspires the following generalization.

Definition. Given a ring R, $x \in R$ is a *unit* iff x has a multiplicative inverse in R.

Note that under this definition, -1 is also a unit in $\mathbb{Z}$.

2. An Interlude on Rings

Here we paused for a refresher on rings. Will proposed a definition: a ring is an abelian group with a second binary operation which is associative and under which the ring is closed. Anya pointed out that we also need the second operation to distribute over the first operation, so that the two operations function analogously to addition and multiplication for the integers. But there's another condition which must be met: a ring must contain the multiplicative identity.[1] To me, fields are more intuitive than rings, and I find it easiest to remember the definition by thinking of a ring as a field without multiplicative inverses. (There's one other distinction: multiplication in a ring is not necessarily commutative.) Here's a formal definition.

Definition. A ring is a set R equipped with two binary operations, $+$ and $\times$, such that:

(1) R is an abelian group under $+$,
(2) $\times$ is associative,
(3) $\times$ distributes with respect to $+$, and
(4) there exists a multiplicative identity (denoted 1).

Date: February 15, 2018.

Based on notes by Ian Banta.

[1] Some authors define a ring without this condition, but this leads to serious problems in applications of the theory.

Naturally, the next notion to define is a subring. Alex ventured that it is a subset of a ring which is itself a ring, but we require slightly more: that its multiplicative identity must be the same as the multiplicative identity of the ambient ring. We also briefly touched on ideals and their parallel with normal subgroups; just as the quotient of a group by a normal subgroup forms a group, the quotient of a ring by an ideal forms a ring.

From here, we returned to units, introducing a bit of notation: for any ring R, we let $R^\times$ denote the set of units of R. For some practice, we found the units for the following rings.

$$\mathbb{Z}^\times = \{\pm 1\} \qquad \mathbb{Z}_3^\times = \{1, 2\} \qquad \mathbb{Z}_6^\times = \{1, 5\} \qquad K[t]^\times = K \setminus \{0\}$$

3. Analogy between $\mathbb{Z}$ and $K[t]$

Using ring-theoretic notation, we can now unify the notions of prime integer and irreducible polynomial: in any factorization into two components, one of the components must be a unit. This hints at a parallel between the structure of $\mathbb{Z}$ and $K[t]$, and we followed this up by listing a number of parallels between the two spaces. Note that in the table below, all except the first two are provable claims. (Also note that $\deg f$ denotes the degree of f. By convention, the degree of the zero polynomial is $-\infty$.)

	$\mathbb{Z}$	$K[t]$
Units (**def**)	$\mathbb{Z}^\times = \{\pm 1\}$	$K[t]^\times = K \setminus \{0\}$
Prime/Irreducible (**def**)	$p \in \mathbb{Z}$ is prime iff $p = ab$ implies a or b is a unit.	$f \in K[t]$ is irreducible iff $f = gh$ implies g or h is a unit.
Factoring	Any $n \in \mathbb{Z}$ can be written as a unit times a product of primes.	Any $f \in K[t]$ can be written as a unit times a product of irreducibles.
Division	For all $a, b \in \mathbb{Z}, b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < \lvert b \rvert$	For all $f, g \in K[t], g \neq 0$, there exists unique $q, r \in K[t]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.
Structure of ideals	$(a, b) := a\mathbb{Z} + b\mathbb{Z} = \big(\gcd(a, b)\big)$	$(f, g) := fK[t] + gK[t] = \big(\gcd(f, g)\big)$
Prime Divisibility Property	p prime and $p \lvert ab \implies p \lvert a$ or $p \lvert b$.	f irreducible and $f \lvert gh \implies f \lvert g$ or $f \lvert h$.

Studying this table, we can compile a dictionary between the worlds of integers and polynomials:

$$\text{prime} \leftrightarrow \text{irreducible}$$
$$\text{magnitude} \leftrightarrow \text{degree}$$
$$\text{positive} \leftrightarrow \text{monic}$$

(The last of these was observed by Daishiro.)

A sketch of the proof of the fourth property in the table was given by Emily and Andrew: one can imagine looking at the integer immediately beneath the rational a/b on the number line. Because of the distribution of integers among rational numbers, we know that the separation is less than 1, so setting q to this integer and r to $a - bq$ gives the desired result.

How does the proof work on the polynomial side? This is a nice exercise. One important observation, due to Eleanor and Anya, is that K being a field is critical. For example, Anya noted that in the case $f = t^2, g = 2t$, there do not exist any polynomials $q, r \in \mathbb{Z}[t]$ with $\deg r < \deg g$ satisfying $f = qg + r$. The proof: we can verify by hand that $q = \frac{1}{2}t$ and $r = 0$ works. But by the property listed in the table, these are the *unique* choices of q and r in all of $\mathbb{Q}[t]$! Hence, there are no possible such choices of q and r in $\mathbb{Z}[t]$.

4. The Game of Fifteen

We next moved on to a seemingly unrelated topic: we played a couple rounds of the 'Game of Fifteen'. The game consists of two people alternating choosing integers from the list $\{1, 2, \ldots, 9\}$; the first person to collect three numbers that sum to fifteen wins. Will and I ended in a draw, but I lost to Eli.

One student noted a similarity to tic-tac-toe. In fact, thinking about it more, we saw that the Game of Fifteen isn't merely *similar* to tic-tac-toe – it's literally the same game, played with different symbols. To see this, consider the 3×3 magic square:

8	1	6
3	5	7
4	9	2

Note that each row, column, and diagonal sum to fifteen. Playing tic-tac-toe on this board is completely equivalent to playing the Game of Fifteen!

In algebraic language, *these two games are isomorphic* – they're the same, apart from the symbols we use to describe them. In the same way, if two algebraic spaces are isomorphic to one another, then they are really the same space – we're just using different symbols to denote their elements / operations.

5. A Final Question

We concluded with a return to polynomials, featuring our favorite polynomial $x^2 + 1 = 0$. Can we solve this polynomial over $\mathbb{F}_3$? (Here $\mathbb{F}_3$ means the same thing as $\mathbb{Z}_3$, but is denoted $\mathbb{F}_3$ to emphasize that it is a field.) Quickly plugging in elements gives

$$0^2 + 1 = 0 + 1 = 1 \quad 1^2 + 1 = 1 + 1 = 2 \quad 2^2 + 1 = 1 + 1 = 2$$

so there is no solution in $\mathbb{F}_3$. When working with this polynomial before in the context of $\mathbb{R}$, we had to 'zoom out' from $\mathbb{R}$ to the larger field $\mathbb{C}$ in order to solve it. This zooming out was done by declaring i to be a solution to $x^2 + 1$ and then declaring $\mathbb{C}$ to be the smallest field containing $\mathbb{R}$ and i. Alex proposed doing the same thing here, forming a new field by adjoining i to $\mathbb{F}_3$. This sounds promising, but alas, there's a fatal flaw. What is it? We'll find out next lecture!