GALOIS THEORY : LECTURE 10

LEO GOLDMAKHER

1. The Degree of a Field Extension

At the end of Lecture 9, we defined the degree of a field extension:

Definition. Given two fields K and L the *degree* of the field extension L/K, written $[L : K]$, is the dimension of L when viewed as a vector space over K.

This definition raised the question of how L can be a vector space over K. In order to answer that question, we look at what the vectors and scalars are. We know that a vector space is an abelian group under addition; since L is a field, its elements form such an abelian group, so we take our 'vectors' to be the elements of L. Next, recall that a vector space is equipped with scalar multiplication. In this case, our scalars are elements of the ground field K. How do we multiply a scalar (an element $k \in K$) by a vector (an element $x \in L$)? We can't multiply the directly, since k might not live inside of L. However, by definition of field extension, there's an embedding $\varphi : K \hookrightarrow L$, so that we have an isomorphic copy of K sitting inside L. This provides a natural way to define how to multiply $x \in L$ by the scalar $k \in K$:

$$kx := \varphi(k)x.$$

To solidify our intuition for the degree of a field extension, we considered a few examples.

Example 1. $[\mathbb{C} : \mathbb{R}] = 2$

To determine the degree of this extension, we notice that $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. This suggests that the set $\{1, i\}$ forms a basis for $\mathbb{C}$. It is clear from how we wrote $\mathbb{C}$ that this proposed basis spans $\mathbb{C}$. Furthermore, as we have shown previously, 1 and i are linearly independent over $\mathbb{R}$. We've thus verified that $\{1, i\}$ forms a basis for the space, so the dimension of $\mathbb{C}$ as a vector space over $\mathbb{R}$ is 2.

Example 2. $[\mathbb{R} : \mathbb{Q}] = \infty$

This extension presents a greater challenge than the previous one. The key observation is that while $\mathbb{Q}$ is countably infinite, $\mathbb{R}$ is uncountable. So, the existence of a finite basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$ would imply that $\mathbb{R}$ is countable. Thus, $\mathbb{R}$ is an infinite dimensional vector space over $\mathbb{Q}$, leading to the conclusion that $[\mathbb{R} : \mathbb{Q}] = \infty$.

Example 3. $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$

For this extension, Wyatt proposed that $\{1, i, \sqrt{2}, i\sqrt{2}\}$ forms a basis for $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}$. To see why this is the case, we will consider a series of extensions.

$$\begin{array}{c} \mathbb{Q}(i, \sqrt{2}) \\ {\scriptstyle 2}\big| \\ \mathbb{Q}(\sqrt{2}) \\ {\scriptstyle 2}\big| \\ \mathbb{Q} \end{array}$$

Date: March 5, 2018.
Based on notes by William Howie.

We observe that the set $\{1, \sqrt{2}\}$ forms a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. This implies that the extension is of degree 2. Similarly, the set $\{1, i\}$ forms a basis for $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$. This implies that this extension is also of degree 2.

Since every element of $\mathbb{Q}(i, \sqrt{2})$ can thus be written as $a + bi$ with $a, b \in \mathbb{Q}(\sqrt{2})$, and each element in $\mathbb{Q}(\sqrt{2})$ can be written as $c + d\sqrt{2}$ with $c, d \in \mathbb{Q}$, we see that we can thus write every element of $\mathbb{Q}(i, \sqrt{2})$ as $q + ri + s\sqrt{2} + ti\sqrt{2}$ with $q, r, s, t \in \mathbb{Q}$. Thus, we have confirmed Wyatt's original proposition, concluding that the degree of the field extension is indeed 4.

This result can be generalized:

Tower Law. *Given fields $L/K/F$, we have $[L : K][K : F] = [L : F]$*

Proof sketch. We will the proof; for the details, see Stewart's presentation in the textbook.

Suppose for the moment that the extensions are both finite, say, $[L : K] = n$ and $[K : F] = m$. Define bases for the extensions as follows:

$$\begin{array}{c} L \\ \text{Basis: } \{a_1,\ldots,a_n\} \longrightarrow \Big| \\ K \\ \text{Basis: } \{b_1,\ldots,b_m\} \longrightarrow \Big| \\ F \end{array}$$

Then it can be shown that

$$\begin{array}{c} L \\ \text{Basis: } \{a_i b_j\} \longrightarrow \Big| \\ F \end{array}$$

whence $[L : F] = nm = [L : K][K : F]$. □

Remark. This theorem holds for infinite extensions as well: $[\mathbb{C} : \mathbb{R}][\mathbb{R} : \mathbb{Q}] = [\mathbb{C} : \mathbb{Q}]$ since $2 \times \infty = \infty$.

Remark. Stewart denotes field extensions by $L : K$ due to its similarity to $[L : K]$. While this is not common notation, we can appreciate that it lets us understand degree as a marker of size. Analogously, if we were to write degree using absolute value bars $|L/K||K/F| = |L/F|$, we see that this looks uncannily similar to the 3^{rd} isomorphism theorem from group theory:

Theorem 1 (Third Isomorphism Theorem)**.** *Let G be a group. If $K \trianglelefteq H \trianglelefteq G$ then $|G/H||H/K| = |G/K|$.*

Actually the theorem states more, namely that the quotient of G/H by H/K is isomorphic to G/K. This strong similarity hints at a deeper connection between normal subgroups and field extensions; we will explore this connection after spring break.

2. Monic Polynomials

Last time, we proved an important result:

Theorem 2. *Given $\alpha \in L/K$. Then*

- *If α is algebraic over K then there exists a monic irreducible polynomial $m_\alpha \in K[t]$ that has α as a root, such that $K(\alpha) \simeq K[t]/(m_\alpha)$. Moreover, $K[\alpha] = K(\alpha)$.*
- *If α is transcendental over K then $K[\alpha] \simeq K[t]$, and (thus) $K(\alpha) \simeq K(t)$.*

Remark. Colloquially, the second part of the theorem asserts that from the point of view of K, a transcendental element α is indistinguishable from an indeterminate; there's no way to describe an α which is transcendental over K using any finite sentence in the language of K.

We call m_α the *minimal polynomial of α over K*. In principle, the minimal polynomial is given to us by the theorem, but how does one actually find m_α? In practice, it's best to think about the minimal polynomial in terms of the following result.

Proposition 3. *Given α algebraic over K. The minimal polynomial m_α is the unique monic nonconstant polynomial in $K[t]$ of minimal degree having α as a root.*

Proof. Suppose that $f \in K[t]$ is a monic polynomial with $f(\alpha) = 0$. From the proof of Theorem 2, we know that $f \in (m_\alpha)$. This implies that $m_\alpha \mid f$, whence $\deg m_\alpha \leq \deg f$. From this, we can conclude that m_α has minimal degree.

It remains to prove uniqueness. Suppose that $\deg m_\alpha = \deg f$, and consider the polynomial $g := m_\alpha - f$. Note that $g(\alpha) = 0$, and that $\deg g < \deg m_\alpha$ (since both m_α and f are monic). I claim $\deg g \leq 0$. Indeed, if $\deg g \geq 1$ then we could renormalize g to be monic, but this contradicts the minimality of the degree of m_α among all monic nonconstant polynomials with α as a root. Thus, g must be a constant, and since it vanishes at α it must equal zero everywhere. We deduce that $f = m_\alpha$, and uniqueness is proved. □

Corollary 4. *Given α algebraic over K, $[K(\alpha) : K] = \deg m_\alpha$.*

Remark. This explains the use of the word 'degree' to describe the dimension of L over K.

Proof. Let $n = \deg m_\alpha$; to conclude the theorem we need to produce a basis of $K(\alpha)$ over K with n elements. Theorem 2 asserts that $K(\alpha) \simeq K[t]/(m_\alpha)$. Our experience tells us that all the elements of the right hand side can be expressed in the form $[f(t)]$ with $\deg f = n - 1$. We therefore conjecture that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K. We proceed in the usual way, showing that these elements are linearly independent over K and span $K(\alpha)$.

> **Span** (Proof suggested by Andrew). Pick any $x \in K(\alpha)$. Since $K(\alpha) = K[\alpha]$, there must exist a polynomial $f \in K[t]$ such that $x = f(\alpha)$. By the division algorithm, we can write $f = qm_\alpha + r$ for some $q, r \in K[t]$ with $\deg r \leq \deg m_\alpha - 1 = n - 1$. Since α is a root of m_α, we deduce that $r(\alpha) = f(\alpha) = x$, thus showing that any element can be written as a linear combination of powers of α with degree at most $n - 1$.
>
> **Linear independence** (Proof suggested by Michael). Suppose $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0$. If any of the c_i were nonzero, then there would exist some largest j for which $c_j \neq 0$. But this would imply that the polynomial $\frac{c_0}{c_j} + \frac{c_1}{c_j}t + \cdots + \frac{c_{j-1}}{c_j}t^{j-1} + t^j \in K[t]$ is monic, has α as a root, and has degree strictly smaller than $n = \deg m_\alpha$, contradicting the minimality of degree of m_α. Thus, we see that all the $c_i = 0$, which shows linear independence of the α^i.

Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)/K$, whence $[K(\alpha) : K] = n = \deg m_\alpha$. □

Thus, the degree of m_α and the degree of $K(\alpha)/K$ are interchangeable. In practice, people simply refer to the *degree of α over K*. Note that this is allowed to be infinite, in the case that α is transcendental over K.

Example 4. We consider the degree of elements over different fields:

(1) The degree of i over $\mathbb{Q}$ is 2. The degree of i over $\mathbb{R}$ is also 2.
(2) The degree of $\sqrt{2}$ over $\mathbb{Q}$ is 2, but the degree of $\sqrt{2}$ over $\mathbb{R}$ is 1.
(3) The degree of e over $\mathbb{Q}$ is infinite, but the degree of e over $\mathbb{R}$ is just 1.

3. The Transcendence of π and e

Stewart provides proofs that π and e are transcendental over $\mathbb{Q}$ in the book. These proofs are technical, but do not require any more background than we already have. Although the proof for π is significantly more challenging than the proof for e, they are somewhat similar. This is perhaps surprising, since it's not immediately clear why the two numbers should be related. It turns out that there's a single theorem which quickly implies the transcendence of both constants, as well as many others. We won't prove the theorem here, since it's beyond the scope of the course, but we state it and see what it implies about π and e.

Theorem 5 (Hermite-Lindemann-Weierstrass)**.** *Given $\alpha_1, \ldots, \alpha_n$ all algebraic and linearly independent over $\mathbb{Q}$. Then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are* algebraically independent *over $\mathbb{Q}$: they cannot be related via any polynomial relation over $\mathbb{Q}$.*

The transcendence of e is an immediate consequence of this: taking $n = 1$ and $\alpha_1 = 1$, we deduce that e is algebraically independent over $\mathbb{Q}$, meaning e doesn't satisfy any polynomial relations over $\mathbb{Q}$.

The transcendence of π is only slightly harder to deduce. Suppose π were algebraic over $\mathbb{Q}$. This would imply that $i\pi$ is also algebraic over $\mathbb{Q}$, whence (letting $n = 1$ and $\alpha_1 = i\pi$) we deduce that $e^{i\pi}$ is transcendental. But this is clearly false, since $e^{i\pi} = -1$. Thus, π must be transcendental.