

Handout 18: Galois theory, part I: linear algebra preliminaries

Okay, we're skipping ahead now, to Section 5.2 of your text. The central theme of this section is the *unsolvability* of a general quintic equation by radical: as explained in the preceding section (5.1), there are "classical" methods using radicals for solving the integer polynomial equations

$$ax^2 + bx + c = 0, ax^3 + bx^2 + cx + d = 0, \text{ and } ax^4 + bx^3 + cx^2 + dx + f = 0.$$

It wasn't until roughly 200 years ago that mathematicians managed to prove (with the fundamental techniques of what we now call abstract algebra) that general radical solutions to fifth-degree polynomial equations over the integers do not exist.

One of our goals is to understand why this is the case, and along the way we'll learn some cool math, particularly that which relates properties of fields and extensions to properties of groups and their normal subgroups.

To begin our next discussion, we're going to need a little bit of linear algebra that we haven't talked about formally in this class:

Definitions. Let k be a field (we'll call it our *scalar field*), and let V be a collection of objects (called *vectors*) such that $(V, +)$ is an abelian group and we may define *scalar multiplication* $k \times V \rightarrow V$ satisfying

- (1) $a(u + v) = au + av$,
- (2) $(a + b)v = av + bv$,
- (3) $(ab)v = a(bv)$, and
- (4) $1_k v = v$

for all $a, b \in k$ and $u, v \in V$. We then call V a *vector space over k* .

Examples.

- (1) If k is any field, then k is a vector space over itself, in which vector addition and scalar multiplication coincide with the addition and multiplication in the field.
- (2) Let $n \in \mathbb{N}$. Then ordinary Euclidean space \mathbb{R}^n is a vector space over \mathbb{R} in the usual way. Can you describe addition and scalar multiplication here?

- (3) Generalizing both (1) and (2) simultaneously, k^n is a vector space over k for any field k and any $n \in \mathbb{N}$.
- (4) Generalizing in a different way, if k is a subfield of K , then K is a vector space over k .

Proof of Theorem 4.31. We proceed much as in the preceding example: find a basis for E over K and a basis for K over k and compute. The hardest thing about the proof is the notation! Here's some room for you to finish it up:

Let's wrap up with one more

Definition. If k and K are fields and K/k is an extension, then $z \in K$ is said to be *algebraic* over k if there is a polynomial in $k[x]$ with root z , and *transcendental* over k otherwise. (If we just say "algebraic" or "transcendental" without reference to a particular k , we generally mean to take $k = \mathbb{Q}$.)

Examples.

- (1) Find an element of \mathbb{R} that is algebraic over \mathbb{Q} .

- (2) It is known (but *very* hard to prove!) that both π and e are transcendental over \mathbb{Q} .
- (3) Prove that $\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is transcendental over $\mathbb{Q}(\sqrt{2})$.

Homework. The following exercises are due on *Friday, April 10th* at 5:00 p.m. None of them are committee problems (don't worry, you'll have a couple of those for next week!)

- (1) Find a field of degree 30 over \mathbb{Q} , and prove that indeed the field has the required degree over \mathbb{Q} .
- (2) Let $k \leq K$ be fields.
 - (a) Let $\alpha, \beta \in K$. Prove that if α and β are algebraic over k , then $\alpha\beta$ is also algebraic over k .
 - (b) Prove that $1_k = 1_K$ is algebraic over k .
 - (c) Let $A = \{\alpha \in K \mid \alpha \neq 0, \alpha \text{ is algebraic over } k\}$. What sort of structure can we claim for A , given parts (a) and (b) and no further proof?
- (3) Decide with whom you will be working for your final presentation. (Recall that you may work either alone or with one other person.)