Math 6140 NOTES: ALGEBRA 2

COLTON GRAINGER
APRIL 17, 2019

These notes were taken in University of Colorado's Math 6140 (Algebra 2) class in Spring 2019, taught by Prof. R. M. Green. I live-TEXed them with `vim`, so there may be typos and failures of understanding. Any mistakes are my own. Please send questions, comments, complaints, and corrections to colton.grainger@colorado.edu. Thanks to `adebray` for the LATEX template, which I have forked from https://github.com/adebray/latex_style_files.

Contents

Lecture 1.

2019-04-15

"The end of Dummit and Foote trailing off into nonsense and pet topics."

Definition 1.1 (Normal basis)**.** A *normal basis* for a Galois extension K/F is an orbit of some element $\alpha \in K$ under the action of $G = \mathrm{Gal}(F/K)$ such that $G(\alpha)$ is a basis for F as a K-vector space.

We'll soon give an existence proof along the lines of "each Galois extension has a normal basis" by producing an such an element α.

Example 1.2. Show that a finite, separable, Galois extension K/F has an element α whose orbit forms a normal basis. ◁

Today we'll jump around a bit, covering odds and ends of 14.2–14.3.

Lemma 1.3. *The natural numbers $d, n \in \mathbb{N}$ satisfy $d \mid n$ if and only if the polynomials $x^d - 1$ and $x^n - 1$ in $\mathbb{Z}[x]$ satisfy $x^d - 1 \mid x^n - 1$.*

Proof. Suppose $d \mid n$. Then let $r = \frac{n}{d}$. Since $x - 1 | x^r - 1$, changing variables $x^d \mapsto x$ produces $x^d - 1 \mid x^n - 1$ in $\mathbb{Z}[x]$. Conversely, if $x^d + 1 \mid x^n - 1$, divide out $x - 1$. Then examine

$$1 + x + \cdots + x^{d-1} | 1 + x + \cdots + x^{n-1} \quad \text{and evaluate at } x = 1.$$

□

Lemma 1.4 (Divisors of 24)**.** *Suppose $a, n \in \mathbb{N}$ are coprime (positive?) integers and $n \mid 24$ and $(a, n) = 1$. Then $a^2 \equiv 1 \pmod{n}$. In particular, $1, 3, 5, 7$ all square to 1 modulo 8.*

Example 1.5 ($x^4 + 1$ is irreducible over $\mathbb{Z}$ but reduces modulo every prime.)**.** Recall that the polynomial $x^4 + 1$ reduces into quadratic factors over $\mathbb{R}$, but is irreducible over $\mathbb{Q}$. (We are guaranteed a root for any cubic polynomial over $\mathbb{R}$ by the intermediate value theorem.) We'll consider $x^4 + 1$ over the finite fields for all odd primes p.

I claim (see 1.4 and 1.3) that

$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2-1} - x.$$

Therefore, for K the splitting field of $x^4 + 1$, we deduce that any root $\alpha \in K$ of $x^4 + 1$ is fixed by Φ^2 where Φ is the Froebenius automorphism. But Φ generates the automorphism group $\langle \Phi \rangle = \mathrm{Aut}()$! Therefore, the degree of $[K : F]$ is at most 2. We conclude that $x^4 + 1$ reduces in $[x]$. ◁

Example 1.6. Here's an alternative argument for 1.5 in the algebraic closure ^{a} of .

- How is one to determine the fixed points of Φ in ^{a}?
- Maybe argue that ^{a} a perfect field (which occurs if and only if the Froebenius map Φ is an isomorphism).
- With each element of ^{a} is a pth root, consider $x^{p^2} - x$, and deduce that $x^4 + 1$ reduces modulo p.

◂

Proposition 1.7. *The following are equivalent.*

- *K/F is Galois.*
- *K/F is separable and has the "one out all out" property.*

Proof. In one direction, recall the we've shown that the minimal polynomial of an element β in a Galois extension K/F is the product of linear factors with constant terms given by the distinct conjugates of β.

In the other, TODO. □

Remark 1.8 (Sketch of proof for the fundmental theorem of Galois theory.). Let K/F be a (separable, finite) Galois extension, with $G = \mathrm{Gal}(K/F)$. Let's chat a bit: how are the subfields of K/F and the subgroups of G in Galois correspondence? As an exercise:

(1) Show that there's an injective functor from Grp into Vect taking subgroups to their fixed subfields.

$$\begin{array}{ccc} K & \text{---} & 1 \\ | & & | \\ E & \text{---} & H \\ | & & | \\ F & \text{---} & G \end{array} .$$

(2) Verify $[K : E] = H$ and $[K : F] = G$, which imply $[E : F] = \frac{|G|}{|H|} = [G : H]$.

(3) Suppose H is the fixing group of the field E. For $\sigma \in \mathrm{Gal}(K/F)$, verify[1] that the fixing group of $\sigma(E)$ is "$\sigma H \sigma^{-1}$".

(4) Exhibit a set bijection $\mathrm{Emb}(E/F) \leftrightsquigarrow \{\text{cosets of } H \leq G\}$, with the cosets of H in G indexed by $\tau \in \mathrm{Gal}(K/F)$ (require that τ restricts to σ on E).

(5) Then

$$\tau^{-1}\sigma \quad \text{is the identity on } E, \text{ so } \quad \sigma H = \tau H.$$

(6) Here's a sketch.

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \xrightarrow{\sigma} \sigma(E) & H \\ | & & | \\ F = \mathbb{Q} & & G \end{array} .$$

◂

Proposition 1.9 (Second isomorphism theorem)**.** *Let K/F be a Galois field extension, with F'/F any other field extension. There's a correspondence $N \leftrightsquigarrow K/F$ and $H \leftrightsquigarrow F'/F$. Then with $H \cap N$ corresponding to KF'/F and HN to $K \cap F'$, we deduce TODO.*

Proposition 1.10 (Intersections of Galois extensions)**.** *Say that K_1/F and K_2/F are Galois over F. Then*

$$\frac{(K_1 \cap K_2)}{F} \quad \textit{and} \quad \frac{(K_1 K_2)}{F} \quad \textit{are Galois} \quad .$$

Corollary 1.11 (Elements that agree on the intersection of Galois groups)**.** *There's a means to lift $\frac{K_1 K_2}{F}$. How?*

How to embed $\mathbb{Q}(\sqrt[3]{2})$ in a Galois extension? There are gross counter examples here, e.g., $x^p - t \in \mathbb{Z}[t][x]$.

[1] If we want to fix the image of E under automorphisms $\sigma(E) = E$ for all σ, then we need "$\sigma H \sigma^{-1} = H$" for all σ, i.e., $H \triangleleft G$.

Definition 1.12 (Galois closure)**.** Say $K \geq E \geq F$ is a tower of field extensions (assume finite and separable). Suppose K/F is maybe not Galois.

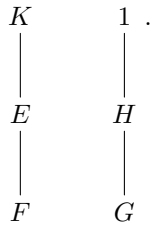
The analogy for groups is the following: we want to find N normal in G, such that $N \leq H$, and N is as large as possible in H. One can take

$$N := \cap_{g \in G} gHg^{-1}$$

to satisfy these requirements.

For fields, then, take the composite of the images of the splitting field Λ for F in K under the action of $\mathrm{Gal}(K/F)$. The composite of all fields in this orbit form the smallest field extension E such that E/F is Galois:

$$E := \cup_{\alpha \in \mathrm{Gal}(K/F)} \alpha^{-1} \Lambda \alpha.$$



Lecture 2.

2019-04-17