6320-001 - SPRING 2021 - WEEKS 11-12 (3/30, 4/01, 4/06, 4/08)

1. The next two weeks in 6320

3/30 – Galois extensions and the fundamental theorem of Galois theory.
4/01 – Cyclotomic fields.
4/06 – Galois groups of polynomials.
4/08 – Solvability in radicals.

The basic results and definitions in Galois theory:
If L is a field and $S \subset \mathrm{Aut}(L)$ is a subset, we write

$$L^S := \{\ell \in L \mid \sigma(\ell) = \ell \; \forall \, \sigma \in S\}.$$

It is simple to check that it is a subfield, called the fixed field of the collection of automorphisms S. We will use this especially when S is a subgroup of $\mathrm{Aut}(L)$.

If L is a field and $M \subset L$ is a subset, we write

$$\mathrm{Fix}(M) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(m) = m \; \forall \, m \in M\}.$$

It is simple to check that it is a subgroup; it consists of all automorphisms of L that act trivially (i.e., restrict to the identity) on M. We will use this especially when M is a subfield.

Theorem (Galois extensions and the fundamental theorem of Galois theory)**.**
For L/K a finite extension, $|\mathrm{Aut}(L/K)| \leq [L:K]$, and the following are equivalent:

1. $[L:K] = |\mathrm{Aut}(L/K)|$.
2. $K = L^{\mathrm{Aut}(L/K)}$,
3. *L/K is separable and normal: that is, if $\alpha \in L$, the minimal polynomial $m_\alpha(x) \in K[x]$ of α over K has $\deg m_\alpha$ distinct roots in L.*
4. *L/K is a splitting field of a separable polynomial in $K[x]$,*

When these equivalent conditions hold, L/K is called a ***Galois extension****. Moreover, if L/K is a Galois extension then there is an inclusion reversing bijection*

$$\begin{array}{rcl} \{\textit{Intermediary field extensions } L \supseteq M \supseteq K\} & \leftrightarrow & \{\textit{Subgroups } \{e\} \leq H \leq \mathrm{Aut}(L/K)\} \\ M & \mapsto & \mathrm{Fix}(M) \\ L^H & \leftarrow\!\shortmid & H. \end{array}$$

Furthermore, for any intermediary extension $L \supseteq M \supseteq K$,

1. $|\mathrm{Fix}(M)| = [L:M]$ *and* $[\mathrm{Aut}(L/K) : \mathrm{Fix}(M)] = [M:K]$.
2. *L/M is Galois and* $\mathrm{Aut}(L/M) = \mathrm{Fix}(M)$,
3. *M/K is Galois if and only if* $\mathrm{Fix}(M)$ *is a normal subgroup, in which case*

$$\mathrm{Aut}(M/K) = \mathrm{Aut}(L/K)/\mathrm{Fix}(M).$$

Finally, if $M_1 \leftrightarrow H_1$, $M_2 \leftrightarrow H_2$, then

$$M_1 M_2 \leftrightarrow H_1 \cap H_2 \text{ and } M_1 \cap M_2 \leftrightarrow \langle H_1, H_2 \rangle.$$

For a Galois extension L/K, we sometimes write $\mathrm{Gal}(L/K)$ in place of $\mathrm{Aut}(L/K)$ and refer to it as the *Galois group* of the extension. If $f(x) \in K[x]$ is a polynomial, the Galois group of f means the Galois group of a splitting field of f.

We record a particularly useful computational corollary :

Corollary 1.1.

1. *If L/K is a Galois extension, and $\alpha \in L$ then the roots of the minimal polynomial $m_\alpha(x) \in K[x]$ of α over K are the orbit $\mathrm{Gal}(L/K) \cdot \alpha$.*
2. *If $f \in K[x]$ is separable then the irreducible factors of f are in bijection with the orbits of the Galois group of f on the roots of f in the splitting field, with each orbit corresponding to the roots of an irreducible factor.*

Proof. Left to the reader. □

We also note a corollary when this is combined with the primitive element theorem proved in the problem on your Week 10 homework:

Corollary 1.2. *If $L = K(\alpha_1, \dots, \alpha_m)$ for $\alpha_i \in L$ separable algebraic over K, then L is a simple extension of K, i.e. $L = K(\alpha)$ for some $\alpha \in L$.*

Proof. Left to the reader (hint: embed L in the splitting field of a separable polynomial over K). □

The following lemma, which is the main ingredient in the proof, is also very useful on its own:

Lemma 1. *If L is a field and $G \subset \mathrm{Aut}(L)$ is a finite subgroup then $[L : L^G] = |G|$.*

In particular, this implies that L/L^G is Galois with group G. The proof of Lemma 1 uses independence of characters to establish $|G| \leq [L : L^G]$ and a primitive version of *descent* for the other inequality; it is elaborated in one of the problems below. We recall the statement of independence of characters, which was covered in Week 6, here:

1.1. **Independence of characters.** If G is a group and L is a field, recall that a *character* of G with values in L is a group homomorphism $G \to L^\times$. We can view a character as an element of the set $\mathrm{Maps}(G, L)$ of all functions on G with values in L, which is an L-vector space.

Theorem (Independence of characters)**.** *If X is a set of distinct characters of G with values in L, then X is a linearly independent set when viewed as a subset of the L-vector space $\mathrm{Maps}(G, L)$.*

Proof. We sketch the proof: It suffices to consider X finite, for which we can argue by induction. The base case is clear since any character maps $1 \in G$ to $1 \in L$. Suppose it is known for $|X| < n$, and consider distinct characters $\chi_1, \dots, \chi_n$. Suppose there is a linear dependence

$$a_1\chi_1 + \ldots + a_n\chi_n = 0.$$

By the inductive hypothesis, the a_i are all non-zero, so we may assume $a_n = 1$. Because $\chi_1 \neq \chi_n$, there exists $h \in G$ such that $\chi_1(h) \neq \chi_n(h)$. Obtain a second dependence by using the change of variables $g \mapsto hg$ on G and simplifying, then subtract off a multiple from the first dependence to obtain a nontrivial dependence between $\chi_1, \dots, \chi_{n-1}$, a contradiction. □

2. Comments and suggested reading

Dummit and Foote, 13.3, 13.6, chapter 14.

3. Homework

Due Tuesday, *April 13*, at 11:59pm on Gradescope
All solutions must be typeset using TeX and submitted via Gradescope; handwritten or late submissions will not be accepted. All exercises and problems submitted must start with the statement of the exercise or problem.

You may work in groups, but you must write up your final solutions individually. Any instances of academic misconduct will be taken very seriously.

Justify your answers carefully!

3.1. **Exercises.** *Complete and turn in ALL exercises*:
Grading scale (for each part of an exercise):
3 points – A correct, clearly written solution
2 points – Right idea, but a minor mistake or not clearly argued
1 point – Some progress but multiple minor mistakes or a major mistake
0 points – Nothing written, totally incorrect, or no substantive progress made towards a solution.

Exercise 1.

(1) Show that $\mathbb{Q}(3^{1/3})/\mathbb{Q}$ is not Galois (here $3^{1/3}$ for the unique cube root of 3 in $\mathbb{R}$).
(2) Show that $K = \mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$ is not Galois (here $\sqrt{3}$ is the positive real square root of 3 and $\sqrt{1+\sqrt{3}}$ is the positive real square root of $1+\sqrt{3}$).
(3) Show that $\mathbb{F}_p(t)[x]/(x^p - t)$ is not a Galois extension of $\mathbb{F}_p(t)$.

Exercise 2. Let $\sigma \in \mathrm{Aut}(\mathbb{C}(t)/\mathbb{C})$ be the unique automorphism fixing $\mathbb{C}$ and sending t to $-t$. Use Lemma 1 to show $\mathbb{C}(t)^{\langle\sigma\rangle} = \mathbb{C}(t^2)$.

Exercise 3. Suppose n is a positive integer and K is a field that contains n distinct nth roots of unity. Write $\mu_n \subset K^\times$ for the subgroup of nth roots of unity, which is abstractly isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

(1) Fix $0 \neq a \in K$ and let L be a splitting field of $x^n - a$. Find a natural injective group homomorphism Gal(L/K) $\hookrightarrow \mu_n$. This identifies $\mathrm{Gal}(L/K)$ with the subgroup of dth roots of unity μ_d for some $d|n$, $d = [L:K]$.
(2) Let α be a root of $x^n - a$ in L. For or $d = [L:K]$ as above, show that $\alpha^d \in K$, and that the minimal polynomial of α is $x^d - \alpha^d$. *Hint: Compare the coefficients of* $x^d - 1 = \prod_{\zeta\in\mu_d}(x-\zeta)$ *and* $m_\alpha(x) = \prod_{\sigma\in\mathrm{Gal}(L/K)}(x - \sigma(\alpha))$.
(3) Factor $x^n - a$ into irreducible polynomials in $K[X]$.

Exercise 4. Show that $x^{p^n} - x \in \mathbb{F}_p[x]$ factors as the product of every monic irreducible polynomial of degree dividing n in $\mathbb{F}_p[x]$.

Exercise 5. Compute the Galois group of $x^4 - 16x^2 + 4$ over $\mathbb{Q}$.

Exercise 6. Let L/K be a Galois extension and suppose f is an irreducible polynomial of degree 5 in $K[x]$. If $f(x)$ has no roots in L, prove that it is irreducible in $L[x]$. *Hint: consider the action of* Gal(L/K) *on the factorization of f in $L[x]$.*

Exercise 7. Let $f(x)$ be a degree 5 polynomial in $\mathbb{Q}[x]$ whose Galois group is not solvable. Let L be a splitting field of f over $\mathbb{Q}$.

(1) Prove that there is a most one field K with $\mathbb{Q} \subset K \subset L$ and $[K:\mathbb{Q}] = 2$.
(2) If α and β are irrational elements in L such that α^2 and β^2 are rational, prove that $\alpha\beta$ is rational.

3.2. **Problems.** *Attempt as many as you have time for, but only turn in one (of your choice).*
Grading scale (for the problem you turn in):
10 points - A correct, complete, and clearly written solution.
8 points - Right idea, but one or two minor mistakes or not clearly argued.
5 points - Some progress but several minor mistakes or a major mistake.
0 points - Nothing written, totally incorrect, or no substantive progress made.
Revision policy: *If you score at least 5 points on the problem you turn in then you will be allowed to submit* **one** *revision to your solution before the final exam (May 3, 10:30am). If the revision is correct, complete, and clearly written then your mark will change to 9 points. This policy only applies to the problem you submit, not to the exercises in the previous section.*

Problem 1 (Symmetric functions)
Let K be a field and let $K(x_1,\dots,x_n)$ be the ring of rational functions in n variables over K, i.e.

$$K(x_1,\dots,x_n) = \mathrm{Frac}K[x_1,\dots,x_n].$$

There is a copy of the symmetric group S_n inside of $\mathrm{Aut}(K(x_1,\dots,x_n)/K)$ acting by permutation of the variables. In this problem, we determine the subfield $K(x_1,\dots,x_n)^{S_n}$ of *symmetric functions.*

(1) We define the elementary symmetric polynomials by

$$\begin{aligned} e_0 &= 1 \\ e_1 &= \sum_{1\le i\le n} x_i \ (= x_1 + x_2 + \ldots + x_n) \\ e_2 &= \sum_{1\le i_1<i_2\le n} x_i x_j \\ \ldots \\ e_n &= \ldots \ (= x_1 \cdot \ldots x_n) \end{aligned}$$

Show that $K(e_1,\dots,e_n) \subset K(x_1,\dots,x_n)^{S_n}$.

(2) Find a monic polynomial f of degree n with coefficients in $K(e_1,\dots,e_n)$ such that $K(x_1,\dots,x_n)$ is the splitting field of f.

(3) Use (2) to deduce that $[K(x_1,\dots,x_n) : K(e_1,\dots,e_n)] \le n!$

(4) Conclude that $K(e_1,\dots,e_n) = K(x_1,\dots,x_n)^{S_n}$ using Lemma 1.

(5) OPTIONAL - NOT GRADED (because I'm not sure what you covered about integral ring extensions last semester!)
Deduce that $K[x_1,\dots,x_n]^{S_n} = K[e_1,\dots,e_n]$.
Hint: use that $K[e_1,\dots,e_n]$ is integrally closed in $K(e_1,\dots,e_n)$.

Remark: This shows any polynomial that is preserved by all permutations of the variables can be expressed as a polynomial in the elementary symmetric polynomials (e.g. $x_1^2 + x_2^2 = e_1^2 - 2e_2$), a fundamental result in invariant theory.

Problem 2 (Constructibility of the regular n-gon)
Read: DF 14.3 and/or the posted excerpt from Courant-Robbins

Definition. A real number $\alpha \in \mathbb{R}$ is *constructible* if a segment of length α can be produced from a segment of length 1 using only a straight-edge and compass.

In the reading, you saw that a straight-edge and compass can be used to perform field operations (addition, subtraction, multiplication, and division). You also saw that they can be used to extract square roots. In a precise sense, this is all that is possible:

Theorem. *A number $\alpha \in \mathbb{R}$ is constructible if and only if there is a a chain of extensions*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$$

such that $\alpha \in K_n$ and $[K_i : K_{i-1}] = 2$.

We admit this theorem without proof for the remainder of the problem.

Example 3.1. $\sqrt{7 + \sqrt{5 + \sqrt{3}/2}}$ is constructible.

Remark 1. In particular, the constructible numbers form a subfield of $\mathbb{R}$, and one can show that it is an *infinite Galois extension* of $\mathbb{Q}$. In this generalization of Galois theory, the Galois group is a *profinite* group (a limit of finite groups – another common example is the p-adic integers $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$). We won't use this statement below.

A regular n-gon is constructible if it can be drawn using only a straight edge and compass (starting with a segment of length 1). For example: the regular 3-gon (equilateral triangle), and regular 4-gon (square) are constructible (you can probably figure out the constructions on your own!). In the rest of this problem, we show

Theorem (Gauss, Wantzel)**.** *The regular n-gon is constructible if and only if*

$$n = 2^k \cdot p_1 \cdot \ldots \cdot p_m$$

for $k \geq 0$ and p_i distinct Fermat primes (that is $p_i = 2^{l_i} + 1$).

Remark 2. One can show that if $2^\ell + 1$ is prime then ℓ is itself a power of 2. Fermat conjectured that

$$2^{2^s} + 1$$

is prime for all $s \geq 0$. This is true for the first few terms: 3, 5, 17, 257, 65537. Euler showed the next term, 4294967297, is composite by staying up late at night doing long division. In fact, there are no other known Fermat primes besides the five listed above – we know the factorization of at least the next few terms in the sequence (they are composite), but we do not know if there are more Fermat primes afterwards!

We proceed to a proof of the theorem in three parts:

1. Observation: the regular n-gon is constructible if and only if $\cos(2\pi/n)$ is a constructible number. You do not need to write anything, but make sure you understand this.
2. When is the order $(\mathbb{Z}/n\mathbb{Z})^\times$ a power of 2?
3. Express $\cos(2\pi/n)$ using roots of unity.
4. Prove the theorem. *Hint: use the Galois theory of cyclotomic extensions.*

Problem 3 (Proof of Lemma 1)

(1) If L/K is an extension, then we may consider L as a K-vector space; we write $\mathrm{End}_K(L)$ for the set of K-vector space endomorphisms of L. We may consider $\mathrm{End}_K(L)$ as an L-vector space via $(\ell \cdot f)(x) = \ell f(x)$. If L/K is finite,

  (a) Show that $\mathrm{End}_K(L)$ has dimension $[L : K]$ as an L-vector space.

  (b) Using independence of characters, conclude that $[L : K] \geq |\mathrm{Aut}(L/K)|$. *Hint: if* $\sigma \in \mathrm{Aut}(L/K)$*, then* $\sigma|_{L^\times} : L^\times \to L^\times$ *is a character of the group* $L^\times$ *with values in* L*!*

(2) Let L be a field, let $G \subset \mathrm{Aut}(L)$ be a subgroup, and let $K = L^G$.

  (a) If V is a K-vector space, then $L \otimes_K V$ is an L-vector space by left multiplication. The action of G on L induces a K-linear action on $L \otimes_K V$:

$$g(\ell \otimes v) = g(\ell) \otimes v.$$

  Show that if $W \subset L \otimes_K V$ is a non-zero L−subspace such that $g(W) \subset W$ for all $g \in G$, then $W \cap 1 \otimes V$ contains a non-zero vector. *Hint: take a nonzero tensor of minimal rank in* W*; if the rank is not one, use the* G*-action to produce a tensor of smaller rank.*

  (b) If we view L as a K-vector space, then $L \otimes_K L$ is an L vector space via left multiplication as in (a). Consider the L-linear map

$$\begin{aligned} L \otimes_K L &\to \mathrm{Maps}(G, L) \\ \ell_1 \otimes \ell_2 &\mapsto (g \mapsto \ell_1 \cdot g(\ell_2)) . \end{aligned}$$

  Show that this map is injective by showing the kernel is preserved by G and then using (a) to obtain a contradiction if it is non-zero.

  (c) Conclude that $[L : K] \leq |G|$.

(3) Combine (1) and (2) to prove Lemma 1.

Remark. Part 2.(a) can be refined to show that $W = L \otimes (W \cap 1 \otimes V)$. In other words, K-subspaces of V are in natural bijection with G-stable L-subspaces of $L \otimes_K V$. This is the fundamental example of *Galois descent*, an important technique in modern algebra that often lets us replace the study of an object (e.g., an algebraic variety) over an arbitrary field with the study of Galois-stable objects over an algebraically closed field.