Wellesley Math Bootcamp
Lecture: Galois Theory

1. Field extensions
2. Algebraic elements over fields, examples. Notation $f|_\alpha$.
3. If $\alpha \in L$, then there is evaluation map $e_\alpha \colon K[x] \to L$ given by $e_\alpha(f) = f|_\alpha$. The kernel is principal ideal so generated by some unique monic polynomial.
4. Proposition: This monic polynomial is irreducible.

   Proof: Suppose that $m_\alpha = fg$. Then $0 = f(\alpha)g(\alpha)$. If $f(\alpha) = 0$, then $f \in (m_\alpha)$ so m_α divides f, i.e. $rm_\alpha = f$. Then $m_\alpha = rm_\alpha g$, so $rg = 1$, so g is a unit. •
5. Notation: We write $K(\alpha) = K[x]/(m_\alpha)$.
6. Observation: Every element of $K(\alpha)$ is of the form $p(\alpha)/q(\alpha)$, where $p, q \in K[x]$.
7. Lemma: If $K(\alpha) : K$ is simple algebraic, every element of $K(\alpha)$ has a unique expression $p(\alpha)$ where p is a polynomial over K and the degree of p is less than the degree of m.

   Proof: Every element in $K(\alpha)$ is of the form $f(\alpha)/g(\alpha)$, where $f, g \in K[x]$ and $g(\alpha) \neq 0$. Since $g(\alpha) \neq 0$, m does not divide g, and since m is irreducible, then $(m, g) = 1$. Hence there are $r, s \in K[x]$ such that $rg + sm = 1$. Hence $r(\alpha)g(\alpha) = 1$. Then $f(\alpha)/g(\alpha) = f(\alpha)r(\alpha) = h(\alpha)$ for some $h \in K[x]$. Let $h = qm + p$, where the degree of p is less than the degree of m. Then $p(\alpha) = h(\alpha)$, so existence is clear.

   To see uniqueness, suppose $f(\alpha) = g(\alpha)$ where both degrees of f and g are less than the degree of m. If $e = f - g$, then $e(\alpha) = 0$ and the degree of e is less than the degree of m. Since m is minimal, we have $e = 0$, so $f = g$. •
8. Examples
   (a) $\mathbb{Q}[x]/(x^2 - 2)$
   (b) $\mathbb{R}[x]/(x^2 + 1)$
   (c) $\mathbb{Q}[x]/(x^2 - 2x - 1)$
   (d) $\mathbb{Z}_3[x]/(x^2 + 1)$
   (e) $\mathbb{Q}[x]/(x^3 - 2)$
9. If m is a monic irreducible polynomial of degree n over $\mathbb{Z}_p$, then $\mathbb{Z}_p[x]/(m)$ has p^n elements.
10. Construct fields of order 8 and 27.
11. Vector spaces, basis
12. Consider basis of $K(\alpha)$, where α is the root of some irreducible polynomial m_α of $K[x]$.
13. Consider the basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.
14. Use of the notation $[L \colon K]$. Definition of finite extension.
15. Definition of algebraic element and algebraic extension.

16. An element α is algebraic over K iff $K(\alpha)\colon K$ is finite.

    Proof: If α is algebraic with minpoly m, then $[K(\alpha)\colon K] = \deg m$. If $[K(\alpha)\colon K] = n$. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis, so $\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ is linearly dependent. Therefore there is a polynomial annihilating α, so α is algebraic.

17. Corollary: If $L\colon K$ is finite, then it is algebraic.

    Proof: If $\alpha \in L$, then $K(\alpha)\colon K$ satisfies $[K(\alpha)\colon K] \leq [L\colon K]$, so is finite. Hence α is algebraic.

18. Converse is false.

19. Tower Law $[L\colon K] = [L\colon M][M\colon K]$.

20. Proposition: Let $L\colon M\colon K$. The minimum polynomial of $\alpha \in L$ over M divides the minimum polynomial of α over K.

21. Apply this to find the minimum polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$.

22. Definition: If $f \in K[x]$ is a polynomial and $L\colon K$ is a field extension, then f *splits over* L if $f = \lambda(x - \alpha_1)\cdots(x - \alpha_n)$, where $\alpha_i \in L$ and $\lambda \in K$.

23. Definition: We say that $L\colon K$ is a *splitting field* for f over K if (1) f splits over L and (2) if $K \subseteq L' \subseteq L$ and f splits over L', then $L' = L$.

24. Theorem: If $f \in K[x]$ splits over L as $f = \lambda(x - \alpha_1)\cdots(x - \alpha_n)$, then $K(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f.

25. Examples:

    (a) $x^2 - 3$ over $\mathbb{Q}$
    (b) $x^2 - \pi$ over $\mathbb{R}$
    (c) $x^2 + \pi$ over $\mathbb{R}$
    (d) $x^3 - 1$ over $\mathbb{Q}$
    (e) $(x^2 - 3)(x^2 + 1)$ over $\mathbb{Q}$
    (f) $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$
    (g) $x^m - 1$ over $\mathbb{Q}$, where $m \in \mathbb{Z}_{\geq 1}$

26. Claim: If $[K(\alpha)\colon K] = n$ and $[K(\beta)\colon K] = m$ are coprime, then $[K(\alpha, \beta)\colon K] = mn$.

27. Example: $x^p - 2$ over $\mathbb{Q}$, where p is prime.

28. Definition of K-automorphism α of L. Define $\mathrm{Gal}(L\colon K)$ or $\mathrm{Gal}(L\colon K)$ to be set of all K-automorphisms of L.

29. Claim: If $L\colon K$ is a field extension, then $\mathrm{Gal}(L\colon K)$ is a group under composition.

30. Terminology: Galois group.

31. Compute $\mathrm{Gal}(\mathbb{C}\colon \mathbb{R})$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})\colon \mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q})$.

32. Need correspondence between subgroups of $\mathrm{Gal}(L\colon K)$ and intermediate subfields of $L\colon K$.

33. Let $\mathcal{G}$ be the set of subgroups of $\mathrm{Gal}(L\colon K)$ and $\mathcal{F}$ be the set of intermediate subfields of $L\colon K$.

34. Want to prove that, if L is the splitting field for an irreducible $f \in K[x]$, then for any two roots α and β of f, there is an element $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.

35. Definition: If $H \leq G = \mathrm{Gal}(L/K)$, then $H^\dagger$ is the subfield of L fixed by H. Then $\dagger\colon \mathcal{G} \to \mathcal{F}$.

36. Remark: Clearly $\langle e \rangle^\dagger = L$. Is $G^\dagger = K$?

37. Examples

    (a) $\mathbb{Q}(\sqrt[5]{3})\colon \mathbb{Q}$ and $G = \langle e \rangle$, so $G^\dagger = \mathbb{Q}(\sqrt[5]{3})$

    (b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

    (c) $\mathbb{Q}(e^{2\pi i/5})$.

38. Proposition: Properties of $*$ and $\dagger$.

    (a) If $H_1 \leq H_2$, then $H_2^\dagger \subseteq H_1^\dagger$. If $\alpha \in H_2^\dagger$, then σ fixes all elements in H_2, so σ fixes all elements of H_1, so $\alpha \in H_1^\dagger$.

    (b) If $M_1 \subseteq M_2$, then $M_2^* \subseteq M_1^*$. If $g \in M_2^*$, then g fixes all elements in M_2, so g fixes all elements in M_2, so $g \in M_1^*$.

    Now remind that for $\mathbb{Q}(\sqrt[5]{3})\colon \mathbb{Q}$, we have $\mathbb{Q}^{*\dagger} = \langle e \rangle^\dagger = \mathbb{Q}(\sqrt[5]{3})$.

    (c) $M \subseteq M^{*\dagger}$. Let $\alpha \in M$. But $M^{*\dagger} = \{\beta \in L\colon \sigma(\beta) = \beta \ \forall \sigma \in M^*\}$.

    (d) $H \subseteq H^{\dagger *}$. Let $h \in H$. But $H^{\dagger *} = \{g \in G\colon g(\alpha) = \alpha \ \forall g \in H^\dagger\}$. (Leave for HW if no time!)

    (e) $M^{*\dagger *} = M^*$. By (c) we have $M \supseteq M^{*\dagger *}$ and by (d) we have $M^* \subseteq M^{*\dagger *}$.

    (f) $H^{\dagger *\dagger} = H^\dagger$. By (d), we have $H^\dagger \supseteq H^{\dagger *\dagger}$. By (c) we have $H^\dagger \subseteq H^{\dagger *\dagger}$.

39. Theorem 11: Let H be a finite subgroup of $\mathrm{Gal}(L/K)$. Then $[L\colon H^\dagger] = |H|$.

40. Recall that, if $L\colon K$ is separable and normal and finite, then $|G| = [L\colon K]$ (Theorem 15). Also we have $[L\colon H^\dagger] = |H|$ (Theorem 11).

41. Do examples with $x^3 - 2$ and $x^4 - 2$.

42. Definition: We say that an extension is Galois if it is normal and separable.

43. Bad examples in which $G^\dagger \neq K$.

44. Theorem 16: Let $L\colon K$ be a finite extension with Galois group G. If the extension is Galois, then K is the fixed field of G, i.e. $G^\dagger = K$.

45. Theorem 19: Let $[L : K] = n$, separable and normal. Recall that $* : \mathcal{F} \to \mathcal{G}$.

    (a) $|\mathrm{Gal}(L/K)| = n$;

    (b) $*$ and $\dagger$ are inverses;

    (c) If $K \subseteq M \subseteq L$, then $[L : M] = |M^*|$ and $[M : K] = |G|/|M^*|$;

    (d) $M : K$ is normal iff M^* is normal in G;

    (e) If $M : K$ is normal, then $\mathrm{Gal}(M/K) \cong G/M^*$.

46. Any finite field must have p^n elements.

    Proof: A finite field must have characteristic p, and so has a subfield of order p generated by the 1 element. So the field is an extension of $\mathbb{Z}_p$, so has p^n elements. •

47. Define exponent of a group, examples

48. Prove that every finite multiplicative subgroup of a field is cyclic.

    Proof: If $\lambda = e(G)$, then $a^\lambda = 1$ for all $a \in G$. But $x^\lambda - 1$ only has at most λ roots, so $|G| \leq e(G)$. But $e(G) \leq |G|$, so $e(G) = |G|$, so there is a generator (requires a tiny bit more work). •

49. Example: $\mathbb{Z}_p^\times$ is cyclic.

50. K is a finite field of p^n elements iff K is a splitting field for the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$.

    Proof: Let K be a finite field of p^n elements. Then K^* is a multiplicative group of $p^n - 1$ elements. So every $a \in K^*$ satisfies $a^{p^n-1} = 1$, so every element $a \in K$ satisfies $a^{p^n} = a$, i.e. every element $a \in K$ is a root of $x^{p^n} - x$. Since this polynomial can have at most p^n roots, the splitting field is exactly K.

    Consider $x^{p^n} - x$ over $\mathbb{Z}_p$. This has exactly p^n roots because it is separable. We will show that these roots form a field L. If $a, b \in L$, then $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$; $(ab)^{p^n} = ab$; $(b^{-1})^{p^n} = b^{-1}$, $(-a)^{p^n} = -a^{p^n} = -a$. So L is a field containing exactly p^n elements. •

51. Let K be a finite field. Then K is a simple extension of $\mathbb{Z}_p$.

    Proof: Since $K^\times$ is cyclic, let u be a generator. Then $K = \mathbb{Z}_p(u)$. •

52. Corollary: Any two groups of order p^n are isomorphic. Notation: $\mathbb{F}_{p^n}$

53. Theorem: If $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $m|n$.

    Proof: There are d basis elements. By counting, $dm = n$.

54. The index $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = m/n$ in this case.

55. Theorem: If $m|n$, we can consider $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

    Proof: Let $d = n/m$. The roots of $x^{p^m} - x$ are all roots of $x^{p^{md}} - x$ by induction. Suppose that a is a root of both polynomials, then raise the second equation by p^m.

56. Claim: Given $\mathbb{F}_{p^m}$ and $d \in \mathbb{N}$, we can find an irreducible polynomial $f \in \mathbb{F}_{p^m}[x]$ of degree d.

    Proof: Let d be given. We know that $\mathbb{F}^*_{p^{md}}$ is cyclic, so choose a generator α. Let $\phi : \mathbb{F}_{p^m}[x] \to \mathbb{F}_{p^{md}}$ be given by $\phi(g) = g(\alpha)$. This ϕ is a surjective ring HM, so $\mathbb{F}_{p^m}[x]/(h) = \mathbb{F}_{p^{md}}$, where h is some irreducible polynomial of degree k. The LHS is a vector space with k basis elements. There are p^m choices for each coefficient, so there are p^{km} elements of the LHS, but the RHS has p^{md} elements, so $d = k$. •

57. Lemma: Let L be a finite field of characteristic p. The Frobenius map $\phi : L \to L$ defined by $\phi(u) = u^p$ is a $\mathbb{Z}_p$-AM.

    Proof: Clearly it is a HM and fixes elements of $\mathbb{Z}_p$. If $\phi(u) = 1$, then $u^p = 1$, so $(u-1)^p = 0$, so $u = 1$. •

58. Theorem: Let $[L:K] < \infty$ and $|K|$ be finite, then $L:K$ is Galois and $\mathrm{Gal}(L/K)$ is cyclic.

Proof: The field L is finite dimensional over K¡ so $|L| = p^n$ for some n. Hence L is a splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. The roots are all distinct, so the extension $L : \mathbb{Z}_p$ is Galois. The Frobenius map $\phi : L \to L$ is a $\mathbb{Z}_p$-AM, so $\phi \in \mathrm{Gal}(L/\mathbb{Z}_p)$. Now ϕ^n is the identity since $\phi^n(u) = u^{p^n} = u$, so $\phi^n = e$. But this is not true for $k < n$, since otherwise $u^{p^k} = u$ for all $u \in L$, a contradiction. Now $\mathrm{Gal}(L/\mathbb{Z}_p) = n$, so $\langle\phi\rangle = \mathrm{Gal}(L/\mathbb{Z}_p)$. Since $\mathrm{Gal}(L/K)$ is a subgroup of $\mathrm{Gal}(L/\mathbb{Z}_p)$, it is cyclic also. •