Galois Theory Recap

Seb Millar

June 1, 2018

1 Lectures

1. Base notions, tower law
2. Finite extns are algebraic, algebraic elements have irred min polys that generate prime ideals
3. $K(\alpha) = K[\alpha]$, $|K(\alpha) : K| = f_\alpha(t)$, Digression on non constructibility (ruler/compass gives quadratic extns)
4. Import Gauss' lemma/eisenstien, irred mod $p \Rightarrow$ irred $/\mathbb{Q}$. finite set of elements alg/K iff they gen finite diml extn/K, finite diml extns are finitetly generated
5. K-homs are inj, K-homs between same diml extns are isoms, define splitting fields (sf's), show extistence (quotient by irred factor to add root+induct)
6. Uniqueness of sf's proof (zorn type proof strat), def: normal extns are when all min polys split, thm that normal iff sf of some poly, finite subgroups of K are cyclic (NB if K finite, prove by classifctn of ab grps&CRT), def of separability ($f(t)$ sep if each irred factor has no reptd roots in sf)
7. $f(t)$ repeated root iff f,f' commmon irred factor so not sep iff $\operatorname{char} K = p$ and $f \in K[t^p]$, more useful sep defs (α sep if min poly sep, L sep if all elts are sep), examples ($\mathbb{Q} \leq L$ alg $\Rightarrow L$ sep $/\mathbb{Q}$, $\mathbb{F}_p(X^p) \leq \mathbb{F}_p(X)$ purely insep), FUND LEMMA $\{K$-homs into $L\} \leftrightarrow \{$roots of f_α in $L\}$
8. Generalise fund lemma to {extns Φ of K-homs ϕ into L}$\leftrightarrow${roots of $\phi(f(t))$ in L}, useful cors, TFAE: (i) $N = K(a_1, \ldots, a_r)$ sep/K (ii) each a_i sep/$K(a_1, \ldots a_{i-1})$ (iii) if L/K large, exists n distinct K homs $N \to L$. Tower of sep exnts is sep
9. THM OF PRIM ELT (fin sep extns are simple, prf: fin take gen of mult grp, inf show $K(\alpha, \beta) = K(\alpha + \lambda\beta)$ for any apart from fintly many bad λ). Trace and Norm (Tr(α) is sum of embeddings of α, N(α) is product)
10. M/K sep then $(m_1, m_2) \mapsto \operatorname{Tr}_{M/K}(m_1 m_2)$ is non degn bilinr form, so Tr : $M \to K$ is surj (prim elt thm, consider disc, vandermond det), PROVE normal iff sf some $f(t)$ (figure out why!!), normal iff normally gentd.
11. $|\operatorname{Aut}_K(M)| = |M : K|$ iff normal and sep (define GALOIS extn/grp), prf shows ($K \leq M \leq L$, M normal/K then $\phi : M \to L$ has $\phi(M) = M$), FUND THM:
    (a) Galois (contravariant) correspondence:
    $$\begin{aligned} \{\text{intermediate subfields } K \leq M \leq L\} &\longleftrightarrow \{\text{subgroups } H \text{ of } \operatorname{Gal}(L/K)\} \\ M &\longmapsto \operatorname{Aut}_M(L) \\ L^H &\longleftarrow\!\shortmid H \end{aligned}$$
    (b) $H \lhd \operatorname{Gal}(L/K) \Leftrightarrow K \leq L^H$ is normal $\Leftrightarrow K \leq L^H$ is Galois
    (c) $H \lhd \operatorname{Gal}(L/K)$ then $\theta : \operatorname{Gal}(L/K) \to \operatorname{Gal}(L^H/K)$ given by $\theta : \sigma \mapsto \sigma|_{L^H}$ is surj, ker H, so
    $$\frac{\operatorname{Gal}(L/K)}{\operatorname{Gal}(L/L^H)} \cong \operatorname{Gal}(L^H/K)$$
12. HEAVY PROOF LECTURE: Artins thm: if $K \leq L$ arb. extn and H fin subgrp of $\operatorname{Aut}_K(L)$, then $M = L^H \leq L$ fin Gal extn and $H = \operatorname{Gal}(L/M)$, ie {finite subgroups of Gal} $\leftrightarrow$ {finite codiml Galois extns} (proof: $\alpha \in L$, show $|M(\alpha) : M| \leq |H|$, then show $M \leq L$ simple (pick $|M(\alpha) : M|$ maximal, show $L = M(\alpha)$, prim elt thm), then $|L : M| \leq |M(\alpha) : M| \leq |H| \leq |\operatorname{Aut}_M(L)| \leq |L : M|$).
    Thm: $K \leq L$ finite $\Rightarrow \left(K \leq L \text{ Galois } \Leftrightarrow L^{\operatorname{Aut}_K(L)} = K\right)$. Proof of Fund thm.

13. Def of Galois group of $f(t) \in K[t]$ is $\mathrm{Gal}(L/K)$ where L is sf of f. $\{$orbits of $\mathrm{Gal}(f)$ on roots of $f\}$ $\leftrightarrow$ $\{$irred factors $g_j(t)\}$: two roots in same orbit iff root of same $g_j(t)$ (NB if f irred then $\mathrm{Gal}(f)$ is transitive). f irred, $\deg(f) = p$ and f has 2 roots in $\mathbb{C} \setminus \mathbb{R}$ then $\mathrm{Gal}(f) \cong S_p$, f sep deg n char $K \neq 2$ then $\mathrm{Gal}(f) \leq A_n \Leftrightarrow D(f)$ is a square in K, $f(t) = t^3 + ct + d \Rightarrow D(f) = -(4c^3 + 27d^2)$ (in general $\mathrm{disc}(t^n + at + b) = (-1)^{\binom{n}{2}}((1-n)^{n-1}a^n + n^n b^{n-1})$, Trans subgroups of S_4: C_4, V_4, D_8, A_4, S_4, Trans subgroups of S_5: $C_5, D_{10}, H_{20}, A_5, S_5$.

14. Mod p reduction ($\mathrm{Gal}(\bar{f}) \hookrightarrow \mathrm{Gal}(f)$ preserves cycle types), FINITE FIELDS: $\mathbb{F}_{p^r}$ is sf of $t^{p^r} - t$ over $\mathbb{F}_p$, so $\mathbb{F}_p \leq \mathbb{F}_{p^r}$ Galois. THM: $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) = C_r$ with Frob Autmphsm as gen. Cor: $\mathbb{F}_p \leq M \leq \mathbb{F}$ finite, $|M| = p^n$, then $\mathrm{Gal}(\mathbb{F}/M) = \langle \varphi^n \rangle$ where φ is Frob map and $M = \mathbb{F}_p^{\langle \varphi^n \rangle}$.

15. Def mth Cyclotomic extn as sf of $t^m - 1$ over K (supposing char $\nmid m$). Note f, f' coprime so roots of f are distinct so form fin. subgroup hence cyclic hence $L = K(\xi)$ simple for some primitive root ξ. Get inj hom $\theta : \mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^*$, sending ith powering map to i. Def cyctmc poly $\Phi_m(t) = \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^*)}(t - \xi^i)$, note $t^m - 1 = \prod_{d|m} \Phi_d(t)$, show Φ_m always coeffs in ring of ints of prime subfield. Show θ is iso iff Φ_m irred.

16. Now cyctmc over $\mathbb{Q}$, thm: Φ_m irred so $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ (note m not necc. prime). Proof uses claim: $p \nmid m \Rightarrow \xi^p$ root of same irred factor. Def cyclic extn as having cyc Gal group, abelian extn if ab Gal group (so over fin fields, all extns are cyc and cyctmc are ab, but 8th cyctmc of $\mathbb{Q}$ is $(\mathbb{Z}/8\mathbb{Z})^*$ cyc non-ab). KUMMER THEORY. Thm: L sf of $f(t) = t^m - \lambda$, char $\nmid m$. Then $\zeta_m \in L$, $\mathrm{Gal}(L/K(\zeta_m)) \hookrightarrow \mathbb{Z}/m\mathbb{Z}$, and f irred/$K(\zeta_m)$ iff $|L : K(\zeta_m)| = m$.

17. Examples using prev thm to find Gal grps. Converse to thm: $K \leq L$ cyclic deg m, K has prim mth root. Then $\exists \lambda \in K$ st $f(t) = t^m - \lambda$ is irred with L sf of f, gentd by some root of f. Such an extn is KUMMER EXTN. Proof uses embeddings lin indep from sheet 3. Def *extn by radicals* if extn is chain of cyc or kummer extns, f *soluble by radicals* if sf is in extn by radicals.

18. Show cubics solble by radicals (consider adjoining disc and ω), then explicitly in practise. Do same for quartics, use 2nd iso thm, def resolvent cubic.

19. Continue for quartics, then discuss general theory for solubility. For chain of fields get chain of gal grps, def group soluble if succesive quotients are abelian. Show grp soluble (ie quotients ab) iff quotients cyclic. Def derived subgrp G' as $[G, G]$ or minml normal subgrp st G/G' ab. Show G/K ab iff $G' \leq K$.

20. Def derived series as chain of derived sbgrps (so quotients ab). Show if G finite, then G soluble iff derived series is eventually trivial (prf shows derived series is fastest descending chain with ab factors). Show (i) $H \leq G$, G soluble $\Rightarrow H$ soluble (ii) $H \lhd G$ then G soluble iff H and G/H both soluble (prf: use prev prop). Hence A_5, S_5 not soluble. Thm: f soluble by radicals iff $\mathrm{Gal}(f)$ soluble (avoiding chars $\leq \deg(f)$). Examples using this to show f deg 5, $\mathrm{Gal}(f) = S_5$ then f not soluble by radicals. Lemma: extns by radicals can be embedded into some galois extn.

21. Prove prev lemma (read properly, lots of exam qs about this stuff and few worked examples). Prove converse of thing, use all previous theory to compute some gal groups.

22. ALG CLOSURE. Def alg closed (all polys split/no non triv alg extns). Def alg closure as alg closed alg extn. Show if $K \leq L$ and all $f \in K[t]$ splits completely over L then L alg closed. Def partial order, total order, chaim, state zorn, show rings have max ideals. Start showing existence of alg closure.

23. Continue showing existence of alg closure. Thm: $\theta : K \to L$ ring hom, $L = \bar{L}$, $K \leq M$ alg extn, then $\exists$ extn $\phi : M \to L$ with $\phi|_K = \theta$. Prf: zorn proof. Show uniqueness of alg closure, use extn of homs and def of alg closure. SYM POLYS. Return to artins thm, use it to talk about about $M = k[x_1, .., x_n]^{S_n} = L^{S_n}$. Def symm polys $s_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \ldots X_{i_n}$ as coefs of $\prod(t - X_i)$, def alg indep (if sensible hom is iso), thm: $M = L^{S_n} = k[s_1, .., s_n]$ and $s_1, .., s_n$ alg indep over K.

24. Proof of prev prop, def trans basis and trans dim, use artin. Show $K[x_1, .., x_n]^{S_n} = K[s_1, .., s_n]$