Galois groups of Polynomials

Def: f(x) & FIXI the Galois gp. of f(x) is Gal(K)F) for K the S.f. of f(x).

f(x) has roots Γ_{11} , r_{n} . $K = F(\Gamma_{11}, ..., r_{n})$. Any element of Gal(K|F) is determined by action on Γ_{1} 's.

Det: H=Sn is called transitive if for all if thre is JEH wi $\sigma(i) = j$

Thun: f(e) EF(x) sep. of degree n, firred. (=) Gal(f) is a transihie Subgroup of Sn.

90284: =>1 follows from what we know about splitting fields: There is OF Gul (X(F) $col \quad \nabla(r, 1 = rj \quad hor \quad any \quad i \neq j.$ EI f(x) reducible, it factors into a product of (dishinet) irreducibles let ri be a coot of one, ri a root of the other. There is no o s.t. $\sigma(r_i) = r_i \implies not transitive.$

Noter even Galois ext' is s.f. at Some iricd. Possible Galois groups: Transitive Subgps of Sn 2 2/22 A3, S3 3 2/42, 2/22×2/22, A4, Sy, D8 TZ/SZ, D.o, Ar, Sr, Z/SZ x Z/4Z S

Note: disc(t1 + 0 = 5 f separable

$$E_{X:} \quad f(x) = \alpha x^{2} t^{6} \times t^{6}$$

$$= \alpha (x - r_{1})(x - r_{2})$$

$$disc(f) = (r_{2} - r_{1})^{2} = (r_{1} t r_{2})^{2} = 4 pr_{1} r_{2}$$

$$= \frac{b^{2} - 4 \alpha c}{\alpha^{2}}$$

Prop: Char(F)
$$\neq 2$$

Gal(f) $\leq A_n \neq 2$ disc(f) = 12
in F.

Cor: $f(z) \in F(x)$ sep. irred choic Chur(F) $\neq 2$

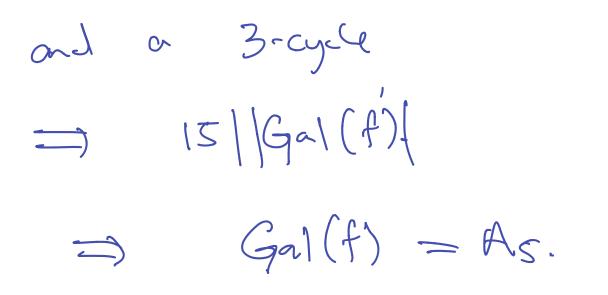
 E_X : $\chi^{5}_{4x+2} \in Q[X]$. Irred. by Elsenstein. Converse basic Calculus to show has $3 \operatorname{real} \operatorname{roots} \Longrightarrow \operatorname{Gal}(f) \cong S_5.$

Thm: (Dedekind) f(x) E R[x] be monie, irred of degæen. For any prime p wl px disc(t) Suggore f(x) factors as $f(x) = f_1(x) - \dots - f_n(x) \mod p$ di = dey (fc) Gal(f) contains a pormutation of type

(d,,--, d.c).

Perof. Too hard for course.

Ex: X-100x-400 lored. b/c it's Icred mod 3. disc(f) = 88000002 $Gal(f) \leq A_{s}$. $\sqrt[7]{x^{5}} = (00 \times -400) = x^{5} \times 12 \times 12$ mod 3 X = (00X - 400 = (xri)(xr3)(xr3xr6xr2)mod 7 Gal(f) contains à 5-cycle

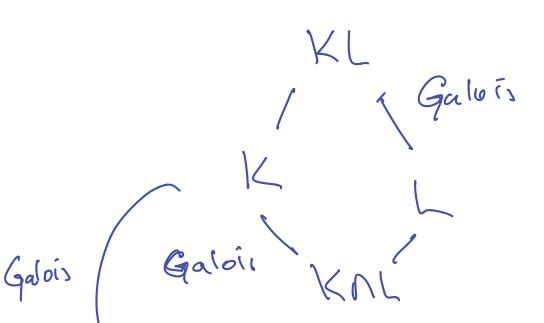


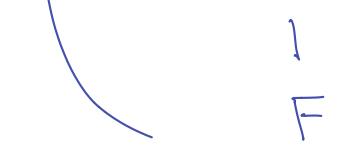
LMFDB assoc. to Ask for number field a polynomicl.

Operations on extensions:

Def: Fi, Fz & F the composite st F, E is denoted FFE is the Smallest subfield of F Containing Fr and F2.

Thm: KIF Galois LIF is any ext Then KL/L is Galois and Gal(KL)L) va Gal(K/KNL)





Jooof: lechne.

K[F, L | F Galois Ihm. Galois/ KL Galois $\left| \right\rangle$ Galois Galois / Galos KNL (Galoja

•
$$KnL | F \text{ is Galois}$$

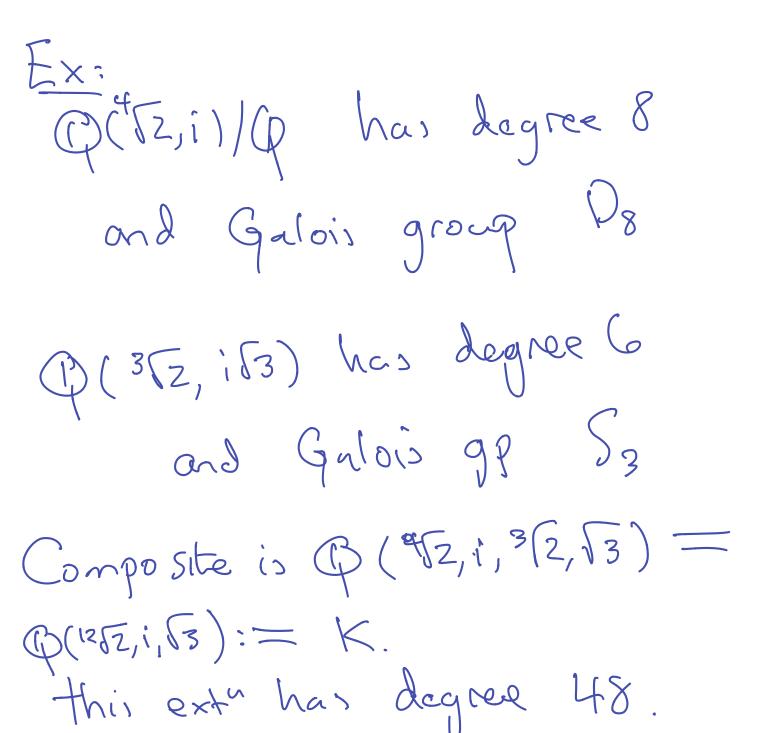
• $KL | F \text{ is Galois}$
• $Gal(KL|F) = 2(G, C) \in Gal(K|F) \times Gal(KL|F) = 2(G, C) \in Gal(K|F) \times Gal(YF)$
• $Gal(YF)$

Proof: 1.) KOLL is sep. ble KIF is sep. fai FEXJ mincred ul a root in Knl. => Foot in Krc spect in K,L blc both room normal => split in KnL normal.

2.) K is s.f. of f(x) onr F L is s.f. of g(x) are F KL is S.f. of Squarefree part of f(x)g(x) on $F \Longrightarrow$ Galois. 3. 10: Gal(KL/F) -> Gal(K/F)×Gul(L/F) Let H = Subgpin the statement. Im(q) ZH is clear. 2/KAL is Galoii, for any

ante. of Kne, there are IL: KALT number of ways to extend it to an automorphism of L. For any GE Gal (KIF) => there are [[: KNI] ways to pick T so that $(\sigma, \mathcal{L}) \in \mathcal{H}$. |Gal(KIF)|.]Gal(L[KNL)| (H(= = |Gal(KL|F)(('check: follows from previous than)

Cor:
$$K/F, L/F$$
 Galois, $KNL = F$
then
 $Gal(KL/F) \subseteq Gal(K/F) \times Gal(L/F).$



43(12, (3, i)) ≤ 16 Q(4/2, 13, 1)21 ((3, 452) (p(3/2))4/ $(\zeta)(53)$ 3 2 1

 $Q(45z,i) \cap Q(sz,is): Q$ divides (and 8=)

divids 2. =) equals 100 2. if degree is 2, then Intersection is a guadratic extⁿ in Q(352, 153). By Gulois corr. the only quadratic Subpeld is Q(153).

 $\bigoplus(4z,i) \land \bigoplus(3z,i)$

 \Rightarrow

= Q(i5)Can check that \$(153)\$ Q(452,i) So this means that degree is 1, so $\mathbb{Q}(4f_{z,i}) \cap \mathbb{Q}(3f_{z,i}f_{3}) = \mathbb{Q}.$ By the corollary, Gal (Q(1252, 1, 53) (Q) \longrightarrow $V_{2} S_{3} \times P_{8}$

Closures: offen times want ext, with certain properties: Separable, normel, Galon, etc. Def: K/F then Freep = { x \epsilon k: x Sep. our f] is a field by HW and we Call Fsep the separable clone of F in K. If K = F we just call it separable Closure. K purely insep-We're seen Forp I Sep F

Prop: if K/F finite, thre is L/k S.t. L/F is normal and [L:K] is minimaal w.r.t. this property.

Proof: $K = F(a_{1,-},a_{n})$ $f(x) = T(m_{a_{1}}(x))$ $\in F[x]$. Take L = s.f. of $f(x)_{n}$

Def: The extension Labour is called the morned closure of K/F.

Note: For general K/F algebrain, need to use def. of normality in terms of field embeddings.

·Sopurable

computations, etc.