Galois tricks

Christmos

Judgement Day

1 Counter-examples

- Inseparable irreducible polynomial: take $K = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$ and consider $X^p - t \in K[X]$. Irreducible by Eisenstein and Gauss' lemma (since t is prime in $\mathbb{F}_p[t]$).
- Non-primitive finite extension: take $K = \mathbb{F}_p(X, Y)$ and $L = \mathbb{F}_p(X^{1/p}, Y^{1/p})$. Then every $x \in L$ is a root of $T^p - x^p \in K[T]$, so any primitive extension has degree at most p, while $[L : K] = p^2$.
- Finite extension $K \subseteq L$ such that $a, b \in L \backslash K$ where a separable over K but b isn't: Take $L = \mathbb{F}_3(a), K = \mathbb{F}_3(a^6), E = \mathbb{F}_3(a^3)$. Take $b = a^3$ Then $[L : K] = 6$ so min poly of a is $T^6 - a^6$ but b is separable.
- Two cycle and p cycle generate S_p
- If its a quintic almost always mod p
- polys of the form $T^p - T + a$ mod p see https://math.stackexchange.com/questions/81583/how-do-i-prove-that-xp-xa-is-irreducible-in-a-field-with-p-elements-when and sheet q ES4 q2 ES3 q13
- know generators of D_{2n}
- can someone remember how j wilson did Q10 (ii) ES4 and summarise here ty
- Finite fields are F_p isomorphic so all polys of degree d split in the finite field of ordr p^d
- if u know thw GG over F_p and the splitting field has degree with factor r, u get the GG over F_p^r for free.
- lets write down solutions to separbility sheet q
- ES2 Q6 https://math.stackexchange.com/questions/1314208/perfect-field-of-characteristic-p

- ES2 Q7 if insperable the min poly of x^p has strictly less degree than that of x so $K(x) \neq k(x^p)$. If $K(x) \neq k(x^p)$ it is ez to show x is inseparable of $k(x^p)$ and so it is inseprable over k as the min polys divide. From this, by the tower law, we deduce that p divides the index of a inseperable extension.

- ES2 Q8 Counting embeddings Lemma

- ES2 Q9 Consider min poly

- Irreducible quadratic mod 2 is only $T^2 + T + 1$. Mod 3 it's $T^2 + 1, T^2 + T - 1, T^2 - T - 1$.

- $\Phi_{np} = \frac{\Phi_n(x^p)}{\Phi_n(x)}$

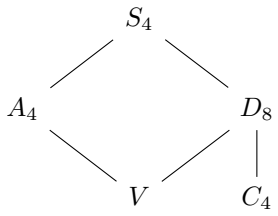
- ES3 Q14 (i) important.Show that an irreducible polynomial $f \in Fq[X]$ of degree d divides $G = X^{q^n} - X$ if and only if d divides n. The splitting field of f is F_{q^d} and so each element of the splitting field and in particular the roots of f (separable) satisfy G so $f|G$. Now for the other direction if the roots of f divide G then F_{q^d} is a subfield of F_{q^n} and apply tower law.

- Cyclotomic: Automorphism of a cyclic group of order n correspond to unit group $(Z/nZ)^x$ by considering image of generator. We can view (injectively) automorphism of a cyclotomic extension by consicering theor action on the roots of unity (or a primitive one) which is a cyclic group hence we get an injection into $(Z/nZ)^x$. This is surjective iff there is a single orbit of all primitive roots of unity because these are exactlly the coprime powers of a generate. (def of primitive is that it has order n). Define cyclo poly. Proof its irreducible over rationals. For prime charisteristuc it will be the orbit of the primitive root under the frob map which is the (multiplicative) order of p in $(Z/nZ)^x$.

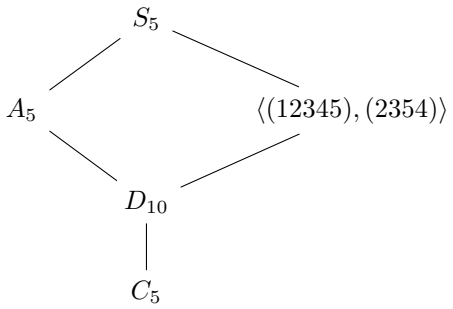
- Kummer: Proof of linear independence of characters. Classification of kummer extensions by looking at what each element rotates the root by. As the galois group is cyclic the order of the GG is the least m st all elements raised to m are the identity. $T^n - a$ reducible iff a a dth power for $d|n$. If $a = y^d$ as we have a primitive dth root of unity we can factor $T^d - y^d$ hence we can factor $(X^m)^d - y^d$. Also f is irreducible iff the GG group above is transitive which happems iff $n = m$. Converse to kummer If Cyclic and root of unit =¿ Kummer (LI of C + Lagrange resolvent produces eigenvalue).

- Trace and norm. Rememeber $P = \sigma_i(x_j))$ to use as a change of basis matric. Also note that ES2 QT gives us trace K(x)/K where $x^p \in k$ is degenerate. Use composition of trace to generalise this degerenacy to all insperabable ectensions. Seperable ectensions have non degernetate trace by linear independence of characters.

- A field K is algebraically closed if every non-constant polynomial over K splits into linear factors over K. A field extension L/K is called an algebraic closure of K if it is algebraic and L is algebraically closed. Countable case, enumarte polynomials and union splitting field i.e. inductively define Li to be a splitting field for fi over L_{i-1}
- any algberaic extension embeds into an algebraic closure. Use a standard zorn arument with poset (extension, embedding). Maximal ideal standard zorn. Existence of alg closure seems too long to come up.
- Cubic: Splits trivial GG, Quadratic C2, Irreducible then check disc. disc $= -4p^3 - 27q^2$ note both negative and the square integer goes with the cube and vice versa
- Quartics: Insert transitive subgroup diagram.
- Quartics: WLOG depress the cubic. Let $y_{12} = x_1 + x_2$ now (as cubic depressed) there is a seperable (check) cubic with roots y_{12}^2,y_{13}^2,y_{14}^2. And we compute it to be $T^3 + 2aT^2 + (a^2 - 4c)T - b^2$. If disc not a square and resolvent irreducible tyehn we have a transitive sungroup not in A_4 with order divisible by 3 so we have S_4.If it is a square and irre is is A_4 by similar reasoning. If reducible and not a square D_4 or C_4 as not in A_4 and S_4 by construction acts tranditively on the roots of the resolvent cubic. Similar for last case V
- Transitive subgroup lattice for S_4



- Transitive subgroup lattice for S_5



- Artin proof. Prove each element satisfies the poly with roots the orbit thus biunding the degree and showuing sperable ectension. Now take a element with max degree it must generate everything ow primitive element thm here means we can find a generator with higher degree. (not really sure why we dont just assume primitive element thm in the first place, actually its bc we dont know its finite) Now apply galois corresponse,
- Fixed field of rational functions is rational functions in the fixed field.Gausses lemma shows they are multiplied by some unit. Order of G in n! so applying n times then the unit is a nth root of unity then $fg^{n!-1}$ and $g^{n!}$ invariant as polys so symmetric sp doen.