1 Quotes

1.1 If it is true, how can you get there?

1.2 First aim for consistency. Then try for speed. - CPS on TOA

1.3 Let's see, is there a just a numerical reason why that would be true? - Kats

on $n|m \iff p^n - 1|p^m - 1$

1.4 Lets see, why is it so compliated? $n = \sum_{d|n} I_d(x)$. Can you use the inherent properties of multiplication (groups) to show it is true? These guys are the total collection of elements that are the elements of order x st x|n in $G = Z_n$

1.5 See how it fails and why it fails, it should suggest how to correct it.

2 Galois

2.1 PROP $GCD(f(x), f'(x)) = 1 \iff f(x), f'(x)$ have no roots in common $\iff$ f(x) has distinct roots in its splitting field

2.2 COR $f(x)$ irreducible $\implies f(x)$ has distinct roots in its splitting field

2.3 DEF Let $F \subseteq K$. $\alpha \in K$ is algebraic over F if there is $f(x) \in F[x]$ s.t. $f(\alpha) = 0$

2.4 RMK Determinant trick: for $\alpha \in K$ gives a polynomial over the base field st $f(\alpha) = 0$

2.5 DEF Let $F \subseteq K$. K is an algebraic extension if all elements of K are algebraic over F

2.6 PROP Let $F \subseteq K$. $\alpha \in K$ is algebraic iff $[F(\alpha) : F] < \infty$

$<=$ If the degree of simple extension is finite, can use determinant trick. $=>$ If α is algebraic, there is a minimal poly in F. So the extension to $F(\alpha)$ is finite. Intuively it says that finite degree extensions are by their nature, algebraic objects. And the reason closely tied to determinants.

2.7 COR Finite degree extension is algebraic

Let $F \subseteq K$ Take any $\gamma \in K$. Consider $F(\gamma) \subseteq K$. It is finite degree extension, so it is algebraic.

2.8 PROP Sufficient condition for simple extension.

Let $Q \subseteq F$ or $|F| < \infty$. If the degree of the extension is finite, it simple ETS show that $F \subseteq F(u, v)$ is simple. Case A B A $Q \subseteq F$ in order for $u + \lambda v$ to not be primitive, λ must satistfy conditions dependent on roots of minimal poly for u and v. Since F infinite, this is not possible. B F finite. The K is cyclic due to gp theory fact. (If $x^n = 1$ has at most n soln. for all n, the G is cyclic. Check Kat's Notes)

2.9 QUES Find an example of a finite extension that is not simple

2.10 Sums and product of algebraic elements are algebraic

2.11 Transitivity of Algebraic

$F \subseteq E \subseteq K$. K algebraic over E and E algebraic over F then K algebraic over F

2.12 Construction of Algebraic Closure

Let $Q \subseteq F$ or $|F| < \infty$. If $|K : F| < \infty$ then $K = F(\alpha)$

2.13 PROP Characterization of finitely many intermediate fields (4-8)

Let $F \subseteq K$ with $|F| = \infty$ $[K : F] < \infty$ Then the extension is simple iff there are only finitely many intermediate fields $F \subset E \subset K$ -> if the extension is simple, there is a minimal poly of α p(x) over F. Take any intermediate field E and consider min poly of α over E <- ETS for $F \subseteq F(u, v)$ has finitely many intermediate fields.

2.14 Remark.

An automorphism fixing F takes root a $f(x) \in F[x]$ to another root. In a primitive field extension, the behavior of α completely describes the behavior of F An homomorphism describes the structure between two algebraic sets An isomorphism says the structure is the same. If an isomorphism maps generators of one Let $F \subseteq K_1$ $F \subseteq K_2$. If K_1 is completely described by roots of a single polynomial, and

2.15 Crucial Prop extension of base field isomorphism to a simple field extension isomorphism

Let $\sigma : F_1 \to F_2$ an isomorphism and $p_1(x)$ min poly of α_1. Let $p_2(x) := p_1(x)^\sigma$, min poly of α_2. Then we can extend to an isomorphism $\overline{\sigma} : F_1(\alpha_1) \to F_2(\alpha_2)$ A special case is that a field extension of any element is identical

2.16 COR Let K be splitting field. If a root of an irreducible poly is in K, then all the roots are in K.

Let K be splitting field for f(x). If p(x) is an irreducible polynomial that has a root in K, then all the roots of p(x) are in K. The proof is very interesting.

2.17 DEF Gal(K) is called Galois if |Gal(K)| = [K:F]

2.18 Characterization of Galois. Let $K = F(\alpha)$, p(x) deg d min poly of α over F. Gal(K) is Galois iff p(x) has d distinct roots in K.

Intuition: Because roots of p(x) go to roots under a $\sigma \in Gal(K/F)$, you need the full set of automorphisms Conversely, the distinct roots give rise to the full set of automoprhisms (Example) of when it fails and how it fails, $\mathbb{Z}_2$ consider $x^2 - 1$.

2.19 TFAE: Let $Q \subset F$. Then TFAE (a) K is Galois over F (b) K is splitting field of p(x) over F. (c) K is splitting field of some $f(x) \in F[x]$ over

2.20 When is Finite Field Extension Galois.

If $|F| < \infty$ (Char(F)=p) ($|K : F| < \infty$ then K is Galois over F Since $K = F(\alpha)$, use the characterization fo Galois. Show that p(x), the minimal poly for α

2.21 Definition. Fixed field of an automorphism or a collection of automorphism.

$K^\sigma := \{k|\sigma(k) = k\}$ $K^H := \{k|\sigma(k) = k, \forall\sigma \in H\}$

2.22 Galois Correspondence Thm.

Let $F \subseteq K$ be finite galois extention.

There is a 1-1 correspondence btw $H \subseteq Gal(K/F)$ and intermediate fields $F \subseteq E \subseteq K$

The correspondnce is given by $H \to K^H \to Gal(K/K^H) = H$?: I understand H is contained in Gal(K/K$^{\mathrm{H}}$), since the maps in H fix K$^{\mathrm{H}}$. But why can't it be more? The correspondence is given by $E \to Gal(K/E) \to K^{Gal(K/E)} = E$?: I understand that E is contained in $K^{Gal(K/E)}$ since the maps in Gal(K/E) already fix E but why can't it be more?

If $H \leftrightarrow E$ corresond, then [G:H]=[E:F]

K is Galois over any intermediate field E

E Galois over F iff Gal(K/E) is normal in Gal(K/F) in which case $Gal(E/F) \cong \dfrac{Gal(K/F)}{Gal(K/E)}$