PRE-MIDTERM AND A FEW PRACTICE PROBLEMS, MATH 505, WINTER 2021

General principle: the expectation is that you are well versed in everything covered in lectures and homework. In particular, know at least one solution to all and any homework problems, **including** worksheets. The list below is not claimed to be comprehensive but I tried to mention most of the topics we covered. If you notice an omission, let me know!

(1) Concepts:
  (a) Field extensions:
    (i) algebraic
    (ii) transcendental
    (iii) normal
    (iv) separable
    (v) purely inseparable
    (vi) Galois
    (vii) cyclic
  (b) Field automorphism
  (c) Galois group
  (d) Splitting field
  (e) Finite field
  (f) Minimal polynomial
  (g) Degree of an extension
  (h) Separable degree of an extension
  (i) Norm and Trace

(2) Theorems:
  (a) Hilbert 90
  (b) Three theorems of Galois Theory
  (c) Existence of algebraic closure
  (d) Extension of automorphisms (see problem 5)
  (e) Equivalent characterizations of normality
  (f) Equivalent characterizations of separability
  (g) Normal basis theorem (statement only)
  (h) Primitive element theorem
  (i) Independence of characters theorem

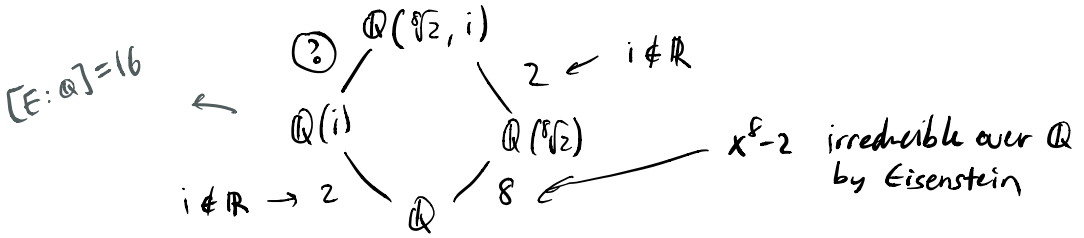
A few practice problems

Disclaimer: this is not a comprehensive list. Once you are confident you've gone over all homework problems, you could try your hand at these, and then continue with an almost unlimited supply in Dummit and Foote.

Problem 1. Let $E = \mathbb{Q}(\sqrt[8]{2}, i)$, $K_1 = \mathbb{Q}(i)$, $K_2 = \mathbb{Q}(\sqrt{2})$, $K_3 = \mathbb{Q}(\sqrt{-2})$. Compute Galois groups of E/K_i for $i = 1, 2, 3$.

Problem 1. $[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}(i)] = \deg(\mathrm{Irr}(\sqrt[8]{2}, \mathbb{Q}(i)))$

$f := \mathrm{Irr}(\sqrt[8]{2}, \mathbb{Q}(i))$ must divide $x^8 - 2$, since $x^8 - 2$ also in $\mathbb{Q}(i)[x]$ that has $\sqrt[8]{2}$ as a root. Consider the diamond. It must be that ? $= 8$, so indeed $f = x^8 - 2$.



E Galois extension of $\mathbb{Q}(i)$, since $f = x^8 - 2$ has ——— distinct roots $\sqrt[8]{2}\,\omega^n$, which are all in E since $\omega := e^{i\pi/4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, and $\sqrt{2} = (\sqrt[8]{2})^4$.

G

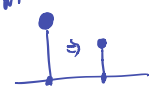
So $|\mathrm{Gal}(E/\mathbb{Q}(i))| = 8$, and $\sqrt[8]{2} \mapsto \sqrt[8]{2}\,\omega^n$, $n \in \{0, \ldots, 7\}$ are all the possibilities hence exactly the elements of G. σ defined as $\sqrt[8]{2} \mapsto \sqrt[8]{2}\,\omega$ generates all of G, since σ^2 maps $\sqrt[8]{2} \mapsto \sqrt[8]{2}\,\omega \mapsto \sqrt[8]{2}\,\omega^2$, etc, so

$\mathrm{Gal}(E/\mathbb{Q}(i)) \cong \mathbb{Z}/8\mathbb{Z}$.

Now for $\mathbb{Q}(\sqrt{2})$. Since $[E:\mathbb{Q}] = 16$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[E : \mathbb{Q}(\sqrt{2})] = 8$.

First, E is splitting field of $x^8 - 2$ over $\mathbb{Q}$. $E \supseteq K$ b/c $x^8 - 2$ indeed splits in E, and $E \subseteq K$ b/c $\sqrt[8]{2}$ obviously gotta be in K, and $\sqrt[8]{2}\,\omega^2 = \sqrt[8]{2}\,i \in K \Rightarrow \frac{\sqrt[8]{2}\,i}{\sqrt[8]{2}} = i \in K$. $x^8 - 2$ separable in E, so E Galois extension of $\mathbb{Q}$

mind picture:



for normality? separability

Important lemmas:

$L \supseteq E \supseteq F$ field extensions. If L/F separable / normal, then L/E separable / normal.

Separable (i.e. all minimal polynomials over base field do not have repeated roots).

$\forall \alpha \in L$, $\mathrm{Irr}(\alpha, F)$ is also $\in E[x]$ that has α as root, so $\mathrm{Irr}(\alpha, E)$ must divide $\mathrm{Irr}(\alpha, F)$. (otherwise their gcd would be smaller degree, ↯ minimality). If $\mathrm{Irr}(\alpha, E)$ has repeat roots, then $\mathrm{Irr}(\alpha, F)$ would too; ↯.

Normal (i.e. if f irreducible over F has ≥ 1 root in L, it has all roots over L (splits over L)).

for (finite algebraic extensions)

Normal $\Leftrightarrow$ splitting field for some polynomial.

see pg 82 of Claus notes

($\Rightarrow$) finite algebraic means $L = F(\alpha_1, \ldots, \alpha_n)$. Letting $m_i(x)$ be $\mathrm{Irr}(\alpha_i, F)$, we know m_i splits over L by normality. Thus, $f = \prod_{i=1}^{n} m_i$ splits over L, and indeed L is splitting field of f, since splitting field of f must contain $\{\alpha_1, \ldots, \alpha_n\}$, but L is smallest field containing $\{\alpha_1, \ldots, \alpha_n\}$.

($\Leftarrow$). property (1) is $\forall \sigma : L \hookrightarrow F^{alg}$ w/ $\sigma|_F = \mathrm{id}$, we have $\sigma(L) = L$.

(1) $\Rightarrow$ normality b/c if $\alpha \in L$, $f = \mathrm{Irr}(\alpha, F)$, define σ to send α to other root of f, fixing F. "extension thingy" (see problem 3 below) gives σ extend to homomorphism $L \to F^{alg}$; so other roots of f must be in L. (↑ injective)

splitting field for some polynomial $\Rightarrow$ (1). Let $\alpha_1 \dots \alpha_n$ be (distinct) roots of f
splitting field of f means $L = F(\alpha_1 \dots \alpha_n)$! (also by injectivity)
If $\sigma : L \to F^{alg}$ fixes F, then $f(\alpha) = 0 \Leftrightarrow f(\sigma(\alpha)) = 0$, so σ permutes roots of α
so $\sigma(L) = \sigma(F(\alpha_1 \dots \alpha_n)) = F(\alpha_{\sigma(1)} \dots \alpha_{\sigma(n)}) = L$.

ANYWAYS, if L/F normal, then L = splitting field of $f \in F[x]$. f also in $E[x]$, so L/E normal too. QED

ANYWAYS, E/k_i are all Galois extensions. So, $|Gal(E/\mathbb{Q}(\sqrt{2}))| = 8$.

~~can we show $E = \mathbb{Q}(\sqrt[8]{2}\, w, \sqrt{2})$? obviously, $\supseteq$, but how about $\subseteq$? we have $(\sqrt[8]{2}\, w)$, don't think so.~~ Well, $x^4 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ has $\sqrt[8]{2}$ as root.

Ok. So $\sqrt[8]{2}$ can be sent to $\pm\sqrt[8]{2}$ or $\pm i\sqrt[8]{2}$. And i can be sent to $\pm i$.
These are only possibilities for where to send $\sqrt[8]{2}$, i & automorphism of $\mathbb{Q}(\sqrt[8]{2}, i)$
completely determined by where it sends $\sqrt[8]{2}, i$, & size of Gal = 8 so there are exactly all the possibilities. Define σ to map $\sqrt[8]{2} \mapsto i\sqrt[8]{2}$, and τ maps $i \mapsto -i$. (order 2)
$i \mapsto i$ $\quad$ $\sqrt[8]{2} \mapsto \sqrt[8]{2}$

Successive applications of σ yield

$$\sqrt[8]{2} \mapsto i\sqrt[8]{2} \mapsto -\sqrt[8]{2} \mapsto -i\sqrt[8]{2} \mapsto \sqrt[8]{2} \quad \text{(so } \sigma \text{ order 4)}$$

Obviously generate whole group $\sigma^0, \sigma^1, \sigma^2, \sigma^3$
$\tau\sigma^0, \tau\sigma^3, \tau\sigma^2, \tau\sigma$. bottom row same as top row except $i \mapsto -i$.

Looking at my "584 midterm Review.pdf" on my website, only group that fits is

$$Gal(E/\mathbb{Q}(\sqrt{2})) \cong D_4$$

Now for $E/\mathbb{Q}(\sqrt{-2})$. By lemmas ? by $E/\mathbb{Q}$ Galois, this is Galois. Again like last time, $[\mathbb{Q}(\sqrt{-2}), \mathbb{Q}] = 2$, so $[E : \mathbb{Q}(\sqrt{-2})] = 8$. ~~inverse of $\sqrt{2}$ in $\mathbb{Q}(\sqrt{-2})$ is $-\frac{1}{2}\sqrt{-2}$~~
If σ maps $\sqrt[8]{2} \mapsto \sqrt[8]{2}\, w^n$ and $i \mapsto i$, then $\sigma(\sqrt{-2}) = \sigma(i\sqrt{2}) = \sigma(i)\,\sigma(\sqrt{2}) = i\,\sigma(\sqrt[8]{2})^4 = i\sqrt{2}\, w^{4n}$
If n even, then $\sigma(\sqrt{-2}) = \sqrt{-2}$. But if n odd, then $w^{4n} = -1$, no good. So for even n,
$\sqrt[8]{2} \mapsto \sqrt[8]{2}\, w^n$, $i \mapsto i$, but if n odd, then $\sqrt[8]{2} \mapsto \sqrt[8]{2}\, w^n$, $i \mapsto -i$. There were only ever 16 possibilities ($\sqrt[8]{2} \mapsto$ 8 possibilities, $i \mapsto$ 2 possibilities), but we threw 8 away. As $|Gal| = 8$, these must be all of them.

Define σ $\quad \sqrt[8]{2} \mapsto \sqrt[8]{2}\, w^2$, $i \mapsto i$
τ $\quad \sqrt[8]{2} \mapsto \sqrt[8]{2}\, w$, $i \mapsto -i$.

Ok wait, don't need σ since $\sigma = \tau^2$?

$$\tau(\sqrt[8]{2}\, w) = \tau(\sqrt[8]{2})\,\tau(w) = \sqrt[8]{2}\, w\, \tau\left(\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i\right)$$
$$= \sqrt[8]{2}\, w \left(\frac{\tau(\sqrt{2})}{2} + \frac{\tau(\sqrt{2})}{2}(-i)\right)$$
$$= \sqrt[8]{2}\, w \left(\frac{(\sqrt[8]{2}\, w)^4}{2} - i\frac{(\sqrt[8]{2}\, w)^4}{2}\right)$$
$$= \sqrt[8]{2}\, w \left(\frac{-\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \sqrt[8]{2}\, w^4 = -\sqrt[8]{2}$$

Ok, so σ, τ both order 4, and $\sigma^2 = \tau^2$.

Finally, we consider $\tau\sigma$ and $\sigma^3\tau$

$$\begin{cases} \tau(\sigma(\sqrt[8]{2})) = \tau(\sqrt[8]{2}\, w^2) = \sqrt[8]{2}\, w\, \tau(w)^2 = \sqrt[8]{2}\, w \cdot w^6 = \sqrt[8]{2}\, w^7 \\ \tau(\sigma(i)) = \tau(i) = -i \end{cases}$$

$$\begin{cases} \sigma^3(\tau(\sqrt[8]{2})) = \sigma^3(\sqrt[8]{2}\, w) = \sigma^2\left(\sqrt[8]{2}\, w^2 \cdot \sigma\left(\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i\right)\right) = \sigma^2\left(\sqrt[8]{2}\, w^2 \cdot \left(\frac{(\sqrt[8]{2}\, w^2)^4}{2} + \frac{(\sqrt[8]{2}\, w^2)^4}{2}i\right)\right) = \sigma\left(\sqrt[8]{2}\, w^2 \cdot w^4\right) \\ \sigma^3(\tau(i)) = \sigma^3(-i) = -i \end{cases}$$
(w in the second parenthesis; $= \sqrt[8]{2}\, w^7$)

and so $\sigma\tau = \sigma^3\tau$. Thus, $Gal(E/\mathbb{Q}(\sqrt{-2})) \cong Q_8$

Problem 2. As part of this problem, you'll prove the "Primitive element theorem".

Let K/k be an algebraic extension.

(1) Assume $K = k(\alpha)$. Show that there are only finitely many distinct subextensions $k \subset F \subset K$.
(2) Assume there are only finitely many distinct subextensions $k \subset F \subset K$. Prove that $K = k(\alpha)$ for some $\alpha \in K$. (Consider the cases when k is finite and infinite separately)
(3) Prove the "Primitive element theorem": if K/k is a finite separable extension then $K = k(\alpha)$.
(4) Give an example of a finite algebraic extension K/k such that there are infinitely many distinct subextensions $K/F/k$. Note: this should also serve as a counterexample to the Primitive element theorem for inseparable extensions.

Problem 3. Prove the "extension thingy" we keep postponing: Let E/K be an algebraic extension, and let $\sigma : K \to K'$ be a non zero field homomorphism. Let $f(x) \in K[x]$ be an irreducible polynomial over K, and $\sigma(f(x)) \in K'[x]$ be the image of f under the homomorphism σ extended to $K[x]$ by sending x to x. Let α be a root of $f(x)$ and β be a root of $\sigma(f(x))$. Prove that there is a homomorphism $\tilde{\sigma} : E \to (K')^{\text{alg}}$ such that $\sigma\downarrow_K = \sigma$ and $\tilde{\sigma}(\alpha) = \beta$.

(1) $E = K[\alpha]$
(2) E/K - finite algebraic extension
(3) E/K - any algebraic extension

Problem 4.[Prelim 2018, 4] Show that the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is Galois and determine its Galois group.

Problem 5.[Prelim 2008, 2] Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

Problem 6.[Prelim 2007, 2 -**This problem is postponed till the Final review. I'll leave it here but don't spend time on it**]

Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

(1) Show that G embeds in the symmetric group S_n.
(2) For each n, give an example of a field K and polynomial f such that $G = S_n$.
(3) What are the possible groups G when $n = 3$. Justify your answer.

Problem 6.[Prelim 2009, 4] Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

(1) Prove that there exists a field extension K of F in which $p(x)$ has a root.
(2) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.
(3) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).
(4) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

Problem 4.

since $\sqrt{2+\sqrt{2}}^2 - 2 = \sqrt{2}$

$\mathbb{Q}(\sqrt{2+\sqrt{2}})$ contains $\mathbb{Q}(\sqrt{2})$. Note $\sqrt{2+\sqrt{2}}$ is root of $(x^2-2)^2-2 = x^4-4x^2+2$, and this is reducible by Eisenstein. So $[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}] = 4$. All roots of $x^4-4x^2+2 =: f$ are $\pm\sqrt{2\pm\sqrt{2}}$, since inverse of $\sqrt{2+\sqrt{2}}$ is $\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2}}$. So it is splitting field of f and f separable in it, so it is Galois. So $|\mathrm{Gal}(E/\mathbb{Q})| = 4$. Only possibilities are $\sqrt{2+\sqrt{2}} \mapsto \pm\sqrt{2\pm\sqrt{2}}$, and b/c size of Gal is 4, these are exactly all the elements of $\mathrm{Gal}(E/\mathbb{Q})$. Ok, then consider σ which maps $\sqrt{2+\sqrt{2}}$ to $\sqrt{2-\sqrt{2}}$, fixing $\mathbb{Q}$. Then,

$$\sigma(\sqrt{2}) = \sigma\left(\sqrt{2+\sqrt{2}}^2 - 2\right) = \left(-\sqrt{2-\sqrt{2}}\right)^2 - 2 = -\sqrt{2}$$

$$\text{so } \sigma\left(-\sqrt{2-\sqrt{2}}\right) = -\sigma\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right) = \sqrt{2}\,\sigma\left(\sqrt{2+\sqrt{2}}\right)^{-1} = -\sqrt{2}\left(\sqrt{2-\sqrt{2}}\right)^{-1} = -\sqrt{2}\left(\frac{\sqrt{2+\sqrt{2}}}{\sqrt{2}}\right) = -\sqrt{2+\sqrt{2}}.$$

Thus, σ is order 4, so it generates all of $\mathrm{Gal}(E/\mathbb{Q})$ so $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$

Problem 5

F finite field, so $|F| = p^m$ for some prime p, $m \in \mathbb{N}$. WTS $\forall n \in \mathbb{N}$, there is irreducible polynomial of degree n $\forall n \in \mathbb{N}$. $F^\times$ has $p^m - 1$ elements, ~~and is cyclic b/c for any $\alpha \in F^\times$~~ An element $\alpha \in F^\times$ has order $d \Rightarrow \alpha^d - 1 = 0$. But we know polynomial $x^d - 1 \le d$ roots. duh So at most d elements have order dividing d. $F^\times$ is abelian, so using classification of finite abelian groups, we have $F^\times \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ where $n_{i+1} \mid n_i$ $\forall i \in \{1, \ldots, s-1\}$. so if $s > 1$, then we will be able to find subgroup $(\mathbb{Z}_{n_s})^2$, i.e. we have at least n_s^2 elements of order dividing n_s, contradicting, meaning $s = 1$, i.e. $F^\times$ cyclic.

in here, we proved the lemma $F^\times$ cyclic $\forall$ finite fields F

Now letting α be generator of $F^\times$, we have $F = \mathbb{F}_p(\alpha)$, since all elements of F are either 0 or $\alpha^{\text{some power}}$, which is in $\mathbb{F}_p(\alpha)$. ($\supseteq$) is clear b/c $\alpha \in F$, and $\mathbb{F}_p \subseteq F$. Thus, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [F : \mathbb{F}_p] = m$. So $\exists$ irreducible polynomial over $\mathbb{F}_p$ of degree m.

So doing this again but writing "F" as a field w/ p^{mn} elements, and "$\mathbb{F}_p$" denoting the original F, I think we prove it?

Existence of finite field of size p^n can be shown as splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$. see Notes of 2/8/21!

Problem 6

$F[x]$ Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

F field, $p \in F[x]$ irreducible.

by UFD ↓ by PID ↓

(1) $\frac{F[x]}{\langle p \rangle}$ is a field since p irreducible $\Rightarrow \langle p \rangle$ prime ideal $\Rightarrow \langle p \rangle$ maximal ideal

so $\frac{F[x]}{\langle p \rangle} = K$ is field extension of $F[x]$ that has a root of p, namely $(x + \langle p \rangle) = \alpha$ $p(\alpha) = p + \langle p \rangle = 0 + \langle p \rangle$

(2) vector space basis of $\frac{F[x]}{\langle p \rangle}$ over $F[x]$ is $\{\langle p \rangle, x + \langle p \rangle, x^2 + \langle p \rangle, \ldots, x^{\deg(p)+1} + \langle p \rangle\}$.

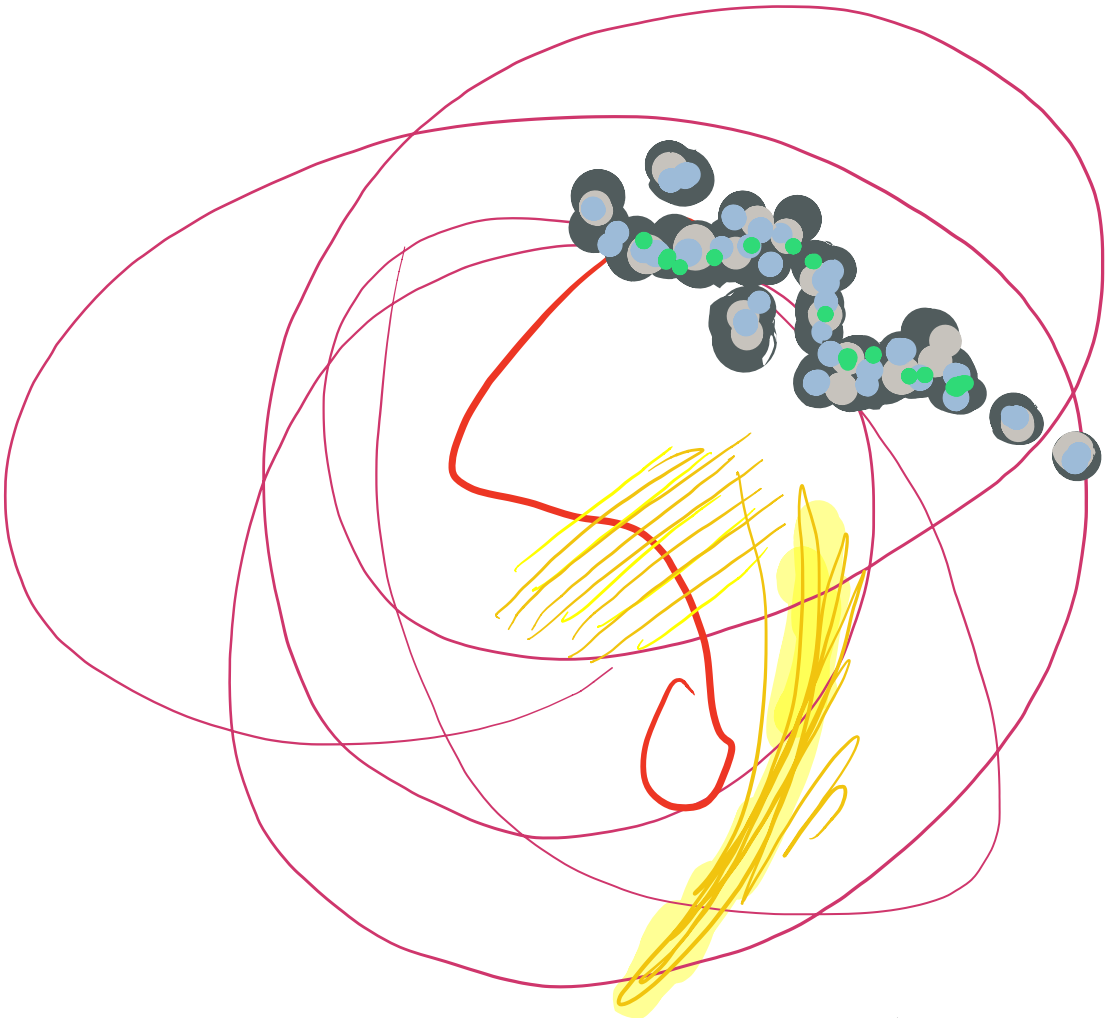
$x^{\deg(p)} + \langle p \rangle$ can be expressed as linear combo of previous, $\because$ p irreducible $\Rightarrow$ can't be less.

(3) $\theta \in K$ is root of p. So $p(\theta) = 0$. So inverse of θ is $\frac{p(\theta) - \text{constant term}}{\theta} \cdot \frac{1}{\text{constant term}}$

(4) $p = x^3 + 9x + 6$ irreducible by Eisenstein over $\mathbb{Q}$. Inverse of $(1+\theta)$ in $\mathbb{Q}(\theta)$

$$\begin{array}{r|l} \theta+1 & \theta^3 + \theta^2 + 9\theta + 6 \\ & \theta^2 - \theta + 10 \\ \hline & -\theta^2 + 9\theta \\ & -\theta^2 - \theta \\ \hline & 10\theta + 6 \\ & 10\theta + 10 \\ \hline & -4 \end{array}$$

$$+\frac{1}{4}(\theta^2 - \theta + 10)$$



Modern art, "Valentines" 2021

Problem 2. As part of this problem, you'll prove the "Primitive element theorem".

Let K/k be an algebraic extension.

(1) Assume $K = k(\alpha)$. Show that there are only finitely many distinct subextensions $k \subset F \subset K$.
(2) Assume there are only finitely many distinct subextensions $k \subset F \subset K$. Prove that $K = k(\alpha)$ for some $\alpha \in K$. (Consider the cases when k is finite and infinite separately)
(3) Prove the "Primitive element theorem": if K/k is a finite separable extension then $K = k(\alpha)$.
(4) Give an example of a finite algebraic extension K/k such that there are infinitely many distinct subextensions $K/F/k$. Note: this should also serve as a counterexample to the Primitive element theorem for inseparable extensions.

Problem 3. Prove the "extension thingy" we keep postponing: Let E/K be an algebraic extension, and let $\sigma : K \to K'$ be a non zero field homomorphism. Let $f(x) \in K[x]$ be an irreducible polynomial over K, and $\sigma(f(x)) \in K'[x]$ be the image of f under the homomorphism σ extended to $K[x]$ by sending x to x. Let α be a root of $f(x)$ and β be a root of $\sigma(f(x))$. Prove that there is a homomorphism $\tilde{\sigma} : E \to (K')^{\text{alg}}$ such that $\sigma\downarrow_K = \sigma$ and $\tilde{\sigma}(\alpha) = \beta$.

(1) $E = K[\alpha]$
(2) E/K - finite algebraic extension
(3) E/K - any algebraic extension

Problem 4.[Prelim 2018, 4] Show that the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is Galois and determine its Galois group.

Problem 5.[Prelim 2008, 2] Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

Problem 6.[Prelim 2007, 2 -**This problem is postponed till the Final review. I'll leave it here but don't spend time on it**]

Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

(1) Show that G embeds in the symmetric group S_n.
(2) For each n, give an example of a field K and polynomial f such that $G = S_n$.
(3) What are the possible groups G when $n = 3$. Justify your answer.

Problem 6.[Prelim 2009, 4] Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

(1) Prove that there exists a field extension K of F in which $p(x)$ has a root.
(2) Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.
(3) If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).
(4) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

pg 594 prop 24 Sec 14.4 of D&F

Problem 2. As part of this problem, you'll prove the "Primitive element theorem". Let K/k be an algebraic extension.

(1) Assume $K = k(\alpha)$. Show that there are only finitely many distinct subextensions $k \subset F \subset K$.
(2) Assume there are only finitely many distinct subextensions $k \subset F \subset K$. Prove that $K = k(\alpha)$ for some $\alpha \in K$. (Consider the cases when k is finite and infinite separately)
(3) Prove the "Primitive element theorem": if K/k is a finite separable extension then $K = k(\alpha)$.
(4) Give an example of a finite algebraic extension K/k such that there are infinitely many distinct subextensions $K/F/k$. Note: this should also serve as a counterexample to the Primitive element theorem for inseparable extensions.

I also used "nptel.ac.in" lecture 12

(1) Let $f = \operatorname{irr}(\alpha, k)$ and suppose F field s.t. $k \subseteq F \subseteq K$ and let $g_F = \operatorname{irr}(\alpha, F)$. Then, $g_F \mid f$. Letting F' be field over k generated by coefficients of g_F. Obviously, $F' \subseteq F$, and b/c g_F irreducible over F, it is irr over F'. But then $[k:F] = \deg g_F = [k:F']$, so F must $= F'$!

So subfields F are exactly those generated by coeff of monic divisors of f in $K[x]$, and there are only finitely many of those.

(2) If k finite, then K is finite, and we know (Problem 5 above) that $k^\times$ is cyclic, so K/k has primitive element.

Now suppose k infinite, w/ finitely many intermediate extensions F. Suppose $\alpha, \beta \in F$, and consider intermediate fields $k(\alpha + \lambda\beta)$ for $\lambda \in k$. k infinite, but # intermediate $< \infty$, so must be $k(\alpha+\lambda_1\beta) = k(\alpha+\lambda_2\beta) =: F$ for $\lambda_1 \neq \lambda_2 \in k$.
so $(\alpha+\lambda_1\beta) - (\alpha+\lambda_2\beta) = (\lambda_1 - \lambda_2)\beta \in F \Rightarrow \beta \in F \Rightarrow \alpha \in F$.
So $k(\alpha,\beta) \subseteq F$, and $\supseteq$ obvious, so any adjoin-2 field $k(\alpha,\beta)$ is actually simple (adjoin-1 field), and continue by induction.

what about K/k infinite extension? ¯_(ツ)_/¯

(3) K/k finite separable, so $K = k(\alpha_1, \ldots, \alpha_n)$. Suffices to prove when $n=2$, extend by induction. So $K = k(\alpha,\beta)$ and we try to look for primitive element $\alpha + \lambda\beta$. Let $m = [K:k]$

We have: $\alpha+\lambda\beta$ generates $K \Leftrightarrow f = \operatorname{irr}(\alpha+\lambda\beta, k)$ deg $= m$
$\Leftrightarrow |\Sigma_{id}| = m \Leftrightarrow \exists$ homomorphism $\sigma_1 = \sigma_m : K \to \bar{k}$ mapping $\alpha+\lambda\beta$ to m distinct places (these places must be roots of f by homomorphism properties) $\Leftrightarrow$
$\sigma_i(\alpha+\lambda\beta) \neq \sigma_j(\alpha+\lambda\beta)$ for $i \neq j \Leftrightarrow \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha)) + \lambda(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0$
$\Leftrightarrow \lambda$ not a root of $g = \prod_{i<j} (\sigma_i - \sigma_j)(\alpha) + x(\sigma_i - \sigma_j)(\beta)$

separability used here

But g has finite degree, k infinite (finite dealt w/ in (2)), so indeed $\exists$ such λ.

(4) If F/k purely inseparable, then char $k > 0$ and k infinite.
(char 0 & finite have no inseparable extensions)

Let $K = \mathbb{F}_p(t,u)$ and $k = \mathbb{F}_p(t^p, u^p)$
$\forall \alpha \in K$, i.e. $\alpha = \frac{f(t,u)}{g(t,u)}$, f,g polynomials, then $\alpha^p = \frac{f(t,u)^p}{g(t,u)^p}$ but by freshman's dream in char p, f^p, g^p are polynomials in t^p, u^p, so $\alpha^p \in k$. I.e. α is root of $x^p - \alpha^p \in k[x]$. Taking $\alpha = t, u$, we see indeed K finite algebraic extension of k.

Claim: $\forall \alpha \in K$, $k(\alpha)$ is intermediate subfield (obviously contains k, and contained by K b/c $\alpha \in K$)
distinctness: try $\alpha = f(y^p)x + y$ for any $f \in \mathbb{F}_p(y)$.

Suppose $k(f_1(u^p)t + u) = k(f_2(u^p)t + u)$. Then, $\alpha, \beta \in k(\alpha)$, so then $t = \frac{\alpha - \beta}{f_1(u^p) - f(u^p)} \in k(\alpha)$, so $u = \alpha - f_1(u^p)t \in k(\alpha)$. Then, $k(\alpha) = K$, i.e. α is primitive element.

This is impossible since it would imply $[K:k] \leq p$, since $\forall \alpha \in K$, $\alpha^p \in k$. But since $\{t^i u^j : i,j \in \{0, \ldots, p-1\}\}$ are linearly independent (as vectors over k), $[K:k] \geq p^2$.

Note also it's $\leq p$, since all polynomials $P(t,u) \in \mathbb{F}_p(t,u)$ i.e. $\mathbb{F}_p[t,u]$ can be written $\sum_{0 \leq i,j \leq p-1} \lambda_{ij} t^i u^j$, for $\lambda_{ij} \in \mathbb{F}_p(t^p, u^p)$ and element $\frac{P}{Q} \in \mathbb{F}_p(t,u)$ equals $\frac{P Q^{p-1}}{Q^p}$ ($\in \mathbb{F}_p[t,u]$, $\in \mathbb{F}_p[t^p, u^p]$) (actually can say $\lambda_{ij} \in \mathbb{F}_p[t^p, u^p]$)
so any $\frac{P}{Q} \in \mathbb{F}_p(t,u)$ can be written as $\sum_{0 \leq i,j \leq p-1} \alpha_{ij} t^i u^j$ for $\alpha_{ij} \in \mathbb{F}_p(t^p, u^p) = k$. I.e. we have shown $\{t^i u^j : 0 \leq i,j \leq p-1\}$ is basis for K over k, so $[K:k] = p^2$.

(taken from MathCounterexamples.net, "Finite extension that contains infinitely many subfields").

D&F proof

(3) Let L be Galois closure of K over k. subfields of K containing k correspond to subgroups of $\mathrm{Gal}(L/k)$ by Gal is correspondence, so # intermediate fields $< \infty$ (since K finite ext of k). So by (2) $\Rightarrow$ simple.

I guess adjoining all roots $\alpha \in \bar{k}$ of some minimal polynomial not already in K.

In char 0, all finite extension of fields is separable, so in char 0, all finite extensions have primitive element.

Problem 3. Prove the "extension thingy" we keep postponing: Let E/K be an algebraic extension, and let $\sigma : K \to K'$ be a non zero field homomorphism. Let $f(x) \in K[x]$ be an irreducible polynomial over K, and $\sigma(f(x)) \in K'[x]$ be the image of f under the homomorphism σ extended to $K[x]$ by sending x to x. Let α be a root of $f(x)$ and β be a root of $\sigma(f(x))$. Prove that there is a homomorphism $\tilde{\sigma} : E \to (K')^{\text{alg}}$ such that $\sigma\downarrow_K = \sigma$ and $\tilde{\sigma}(\alpha) = \beta$.

(1) $E = K[\alpha]$
(2) E/K - finite algebraic extension
(3) E/K - any algebraic extension

(1)

math.stackexchange.com

Fact. Let $f : K \to \Omega$ be a homomorphism of fields were Ω is algebraically closed. Assume that α is an element of some algebraic extension field L of K. Then there exists a homomorphism of fields $\tilde{f} : K[\alpha] \to \Omega$ such that $f(z) = \tilde{f}(z)$ for all $z \in K$.

Proof. Let $m(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ be the minimal polynomial of α. Consider the polynomial

$$\overline{m}(x) = \sum_{i=0}^{n} f(a_i)x^i \in \Omega[x].$$

Because Ω is algebraically closed, there exists an element $\beta \in \Omega$ such that $\overline{m}(\beta) = 0$. Consider the mapping

$$F : K[x] \to \Omega, p(x) = p_0 + p_1 x + \cdots p_t x^t \mapsto \sum_{i=0}^{t} f(p_i)\beta^i.$$

This is the composition of two mappings. The extension of f to a map between polynomial rings $K[x] \to \Omega[x]$ followed by evaluation of polynomials in $\Omega[x]$ at β. Both of these mappings are homomorphism of rings. Thus the same holds for their composition F. We see that the irreducible polynomial $m(x)$ is in the kernel of F. Hence the ideal $I \subset K[x]$ generated by $m(x)$ is also contained in $\ker F$. But irreducibility of $m(x)$ implies that I is a maximal ideal of $K[x]$, so we can conclude that $I = \ker F$. Thus F induces an isomorphism $\overline{F}$ from $K[x]/I$ to a subring of Ω. Here $K[x]/I$ is a field isomorphic to $K[\alpha]$. Composing the inverse of that isomorphism gives us the desired homomorphism

$$\tilde{f} : K[\alpha] \cong K[x]/I \to \Omega.$$

Q.E.D.

math.stackexchange.com

Your claim follows from this by a typical application of Zorn's Lemma. Consider the set E of pairs (ℓ, ϕ), where ℓ is a field such that $k \subseteq \ell \subseteq k'$ and ϕ is a homomorphism of fields $\phi : \ell \to \Omega$ such that $\phi(z) = g(z)$ for all $z \in k$. We say that (ℓ', ϕ') is *an extension of* (ℓ, ϕ), if $\ell \subseteq \ell'$ and $\phi'(z) = \phi(z)$ for all $z \in \ell$. Denote $(\ell, \phi) \prec (\ell', \phi')$. Clearly this is a partial order of E: if $(\ell, \phi) \prec (\ell', \phi')$ and $(\ell', \phi') \prec (\ell'', \phi'')$ then $(\ell, \phi) \prec (\ell'', \phi'')$.

Claim. Every chain in E has an upper bound.

Proof. If $C = \{(\ell_i, \phi_i) \mid i \in I\}$ is a chain in E, then let

$$k_C = \bigcup_{i \in I} \ell_i \subseteq k'$$

be the union of the fields occuring in the chain C. For any $z \in k_C$ we define $\phi_C(z)$ as follows. The element z belongs to at least one of the fields $\ell_i, i \in I$. We declare $\phi_C(z) = \phi_i(z)$. This is well-defined, because if we also have $z \in \ell_j$ for some $j \in I, j \neq i$, then by the chain property we have either $(\ell_i, \phi_i) \prec (\ell_j, \phi_j)$ or $(\ell_j, \phi_j) \prec (\ell_i, \phi_i)$. In either case this implies that $\phi_i(z) = \phi_j(z)$.

Furthermore, the mapping ϕ_C is a homomorphism of fields. For if $z_1, z_2 \in k_C$ are arbitrary, then $z_1 \in \ell_i$ and $z_2 \in \ell_j$ for some $i, j \in I$. Again, one of the fields ℓ_i, ℓ_j contains the other, so the homomorphic condition follows from well-definedness of ϕ_C and the fact that the "bigger" one, either ϕ_i or ϕ_j, is a homomorphism.

Clearly $(\ell_i, \phi_i) \prec (k_C, \phi_C)$ for all $i \in I$, so the pair (k_C, ϕ_C) is an upper bound of the chain C. Q.E.D.

The main claim follows from this. By Zorn's Lemma the set E has a maximal element (ℓ_M, ϕ_M). If here ℓ_M were a proper subfield of k', then we would have that k' is an algebraic extension of ℓ_M. Hence the **Fact** applied to $K = \ell_M$ and to any element $\alpha \in k' \setminus \ell_M$ would allow us to further extend the homomorphism ℓ_M to the field $\ell_M[\alpha]$ contradicting the maximality of (ℓ_M, ϕ_M). Thus $\ell_M = k'$, and the homomorphism ϕ_M is your g'.

credit to
Jyrki Lahtonen on MSE.

Hilbert Thm 90 (additive one for Trace). (see pg 584 D&F).

K Galois extension of F, w/ cyclic Galois group generated by σ (size n). Let $\alpha \in K$. WTS

$$Tr_{K/F}(\alpha) = 0 \iff \alpha = \beta - \sigma(\beta) \text{ for some } \beta \in K.$$

($\Leftarrow$): $Tr_{K/F}(\alpha) = Tr_{K/F}(\beta) - Tr_{K/F}(\sigma(\beta))$ (additivity of norm) $= \sum_{\tau \in Gal(K/F)} \tau(\beta) - \sum_{\tau \in Gal(K/F)} \tau(\sigma(\beta))$ (lemma 3 HW4). But $Gal(K/F)$ cyclic generated by σ, so this is

$$\sum_{i=1}^{n} \sigma^i(\beta) - \sum_{i=1}^{n} \sigma^{i+1}(\beta) = \sigma(\beta) - \sigma^{n+1}(\beta) = \sigma(\beta) - \sigma(\beta) = 0$$

($\Rightarrow$): If $\exists \theta \in K$ s.t. $Tr_{K/F}(\theta) \neq 0$, then consider

$$\beta = \frac{1}{Tr_{K/F}(\theta)} \left(\alpha\sigma(\theta) + (\alpha + \sigma(\alpha))\sigma^2(\theta) + \text{---} + (\alpha + \text{---} + \sigma^{n-2}(\alpha))\sigma^{n-1}(\theta) \right)$$

Since $Tr_{K/F}(\theta) \in F$ (prop 4 HW4) and $Tr_{K/F}$ additive, we have $\sigma(\beta)$ is

$$\sigma(\beta) = \frac{1}{Tr_{K/F}(\theta)} \left(\sigma(\alpha)\sigma^2(\theta) + (\sigma(\alpha) + \sigma^2(\alpha))\sigma^3(\theta) + \text{---} + \underbrace{(\sigma(\alpha) + \text{---} + \sigma^{n-1}(\alpha))}_{= Tr_{K/F}(\alpha) - \alpha = -\alpha} \underbrace{\sigma^n(\theta)}_{\theta} \right)$$

and so $\beta - \sigma(\beta)$ is

$$\beta - \sigma(\beta) = \frac{1}{Tr_{K/F}(\theta)} \left(\alpha\sigma(\theta) - \alpha\sigma^2(\theta) + \text{---} + \alpha\sigma^{n-1}(\theta) + \alpha\theta \right)$$

$$= \frac{1}{Tr_{K/F}(\theta)} \alpha \, Tr_{K/F}(\theta) = \alpha.$$

So all that's left is to show $\exists \theta \in K$ w/ $Tr_{K/F}(\theta) \neq 0$. Well, by linear independence of characters, b/c $\sigma^0, \text{---}, \sigma^{n-1}$ are distinct homomorphisms from $G = K^\times$ to $L^\times = K^\times$ (i.e. taking the field $L = K$), $\sum_{i=0}^{n-1} \sigma^i$ is not identically 0, so there must $\exists \theta$ s.t. $Tr_{K/F}(\theta) \neq 0$ and we are done.

HW2 purely inseparable extensions fixes / review.

If L/F purely inseparable

L/E / f purely inseparable

$\operatorname{Irr}(\alpha, E) \mid \operatorname{Irr}(\alpha, F)$

$\| $

$(x-\alpha)^{p^n}$ we know from previous part of HW2

$\Rightarrow \operatorname{Irr}(\alpha, E)$ must be of the form $(x-\alpha)^{p^m r}$ where $p \nmid r$ (I think this suffices to show $\operatorname{Irr}(\alpha, E)$ not separable ???)

But $(x-\alpha)^{p^m r} = (x-\alpha)^{p^m}(x-\alpha)^r$

Then, by minimality, $\alpha^k \notin F$ $\forall k$ s.t. $1 \leq k < p^m r$ since then

then would be polynomial w/ α as root w/ deg $< p^m r = \deg(\operatorname{Irr}(\alpha, E))$.

[stuff on the way to showing $\alpha \in L \setminus F$ (L/F purely inseparable extension)

$\Leftrightarrow \alpha^{p^n} \in F$ $(\exists n \in \mathbb{N})$