1. (August 2014 Problem 5) It is well-known that if H_1 and H_2 are two subgroups of a group G, then the index $[G : H_1 \cap H_2]$ is at most $[G : H_1][G : H_2]$. But the analogous statement for field extensions is not true.

(a) Let K be the splitting field of $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$. Give an example of two subfields L_1 and L_2 of K such that K/L_1 and K/L_2 are both quadratic extensions, but $K/(L_1 \cap L_2)$ has degree greater than 4.

Galois Extension Property:
Let $\varphi: L \to K$ be a map of fields. Let $f \in L[x]$ be irreducible, let α be a root of f (not necessarily in L), and let α' be a root of $\varphi(f) \in K[x]$. Then there is a map $\tilde{\varphi}: L(\alpha) \to K(\alpha')$ with $\tilde{\varphi}|_L = \varphi$.
In other words, φ induces a map
$\tilde{\varphi}: L[x]/f \longrightarrow K[x]/\varphi(f)$
Moreover, if φ is an isomorphism, then so is $\tilde{\varphi}$.

Splitting Field
The splitting field of a polynomial with coefficients in a field is the smallest field extension of that field over which the polynomial decomposes into linear factors.

The splitting field of $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$ is the splitting field of the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$. The minimal polynomial of $2^{1/3}$ is x^3-2, which has roots $2^{1/3}$, $\omega 2^{1/3}$, $\omega^2 2^{1/3}$, where ω is a primitive cube root of unity. Since K is the smallest extension which contains these roots, and since each root is contained in $\mathbb{Q}(2^{1/3}, \omega)$, it follows that $K \subseteq \mathbb{Q}(2^{1/3}, \omega)$. Since $\omega = \frac{\omega^2 2^{1/3}}{\omega 2^{1/3}} \in K$, and $2^{1/3} \in K$, we also get the reverse inclusion, and conclude that $K = \mathbb{Q}(2^{1/3}, \omega)$.

Note that the degree of $K/\mathbb{Q}$ is 6. We will find subfields L_1, L_2 of K so that K/L_1 and K/L_2 are quadratic extensions, with $L_1 \cap L_2 = \mathbb{Q}$.

$\mathbb{Q}(2^{1/3})/\mathbb{Q}$ has degree 3, and $\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(2^{1/3})$ has degree 2 (the minimal polynomial of ω over $\mathbb{Q}(2^{1/3})$ is x^2+x+1)

Define $L_1 = \mathbb{Q}(2^{1/3})$, $L_2 = \mathbb{Q}(\omega 2^{1/3})$. The minimal polynomial of $2^{1/3}$ and $\omega 2^{1/3}$ over $\mathbb{Q}$ is x^3-2, so the extensions $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ both have degree 3, which implies K/L_1 and K/L_2 are both quadratic extensions.

$\mathbb{Q} \subseteq L_1 \cap L_2 \subseteq L_i$, and $L_i/\mathbb{Q}$ has degree 2.

Now $L_1 \cap L_2$ is a subfield of both L_1 and L_2, and so either $L_1 \cap L_2 = \mathbb{Q}$, or $L_1 \cap L_2 = L_1 = L_2$. Since $L_1 \subseteq \mathbb{R}$, but $L_2 \not\subseteq \mathbb{R}$, we conclude that $L_1 \cap L_2 = \mathbb{Q}$, and so $K/L_1 \cap L_2$ has degree 6.

(b) Let K be the field of rational functions $\mathbb{C}(x)$. Give an example of two subfields L_1 and L_2 of K such that K/L_1 and K/L_2 are both quadratic extensions and such that $K/(L_1 \cap L_2)$ has *infinite* degree.

Define $L_1 = \mathbb{C}(x^2)$, $L_2 = \mathbb{C}(x^2+1)$. Then x satisfies the polynomials $t^2 - x^2 \in L_1[t]$ and $t^2 + t - x^2 - x \in L_2[t]$, so the degrees of K/L_1 and K/L_2 are each at most 2.

Since $x \notin L_1$ and $x \notin L_2$, the extensions cannot have degree 1, and so K/L_1 and K/L_2 are both quadratic.

Nonconstant rational functions in L_1, L_2 have degree ≥ 2

$K = L_i(x)$, so the degree of the minimal polynomial of x over L_i is the degree of the extension K/L_i.

An element of $L_1 \cap L_2$ can be written $\frac{f(x^2)}{g(x^2)} = \frac{h(x^2+x)}{p(x^2+x^2)}$, where $f, g, h, p \in \mathbb{C}[t]$, and where each rational function is written in lowest terms. Then we can say $f(x^2) = h(x^2+x)$, which implies f and h are constant functions, since any nonconstant polynomial of x^2+x will necessarily have an odd-degree term. By the same reasoning, we can say that g and p are both constant, and we conclude that the only functions in $L_1 \cap L_2$ must be constant, so $L_1 \cap L_2 = \mathbb{C}$. Thus $K/L_1 \cap L_2$ has infinite degree.

Note that we are only assuming that $\frac{f(t)}{g(t)}$ and $\frac{h(t)}{p(t)}$ are in lowest terms, i.e. that the rational functions in $\mathbb{C}(t)$ are reduced. However, this actually implies that $\frac{f(x^2)}{g(x^2)}$ and $\frac{h(x^2+x)}{p(x^2+x)}$ are reduced.

2. (January 2015 Problem 5) Let L/K be a finite extension of fields whose degree $p = [L : K]$ is a prime number. Let σ be an automorphism of L over K (that is, an element of the Galois group $Gal(L/K)$, $\sigma \neq id$). Suppose that σ is diagonalizable over K (that is, there is a basis of L as a K-vector space consisting of eigenvectors for σ). Show that L is the splitting field of the polynomial $x^p - a$ for some $a \in K$.

We will not assume that L/K is a Galois extension, so let $\sigma \in Aut(L/K)$. Then the order of σ must be at most p, since $|Aut(L/K)| \leq [L:K] = p$. Let $n > 1$ be the order of σ, so $\sigma^n = id$. This implies that the eigenvalues of σ are n^{th} roots of unity. We will show that each n^{th} root of unity occurs as an eigenvalue, and then show that $n = p$.

If E, L are finite extensions of F, then the number of F-homomorphisms $E \to L$ is at most $[E:F]$. In particular, the order of $Aut(E/F)$ is at most $[E:F]$.

Let $\zeta \neq 1$ be an eigenvalue of σ with eigenvector a. Then $a \in K - L$, since σ fixes L. Since the degree of L/K is p, the minimal polynomial of a must have degree p. $K \subseteq K(a) \subseteq L$

Since eigenvectors form a basis for L, and since $\sigma \neq id$, this must exist.

This implies that $\{1, a, \dots, a^{p-1}\}$ forms a linearly independent set, and thus they must form a basis for L as a vector space over K. Now since $\sigma a = \zeta a$, we have $\sigma a^m = (\sigma a)^m = \zeta^m a^m$, and so in particular, a^p is an eigenvector with eigenvalue ζ^p.

Now let $\ell = p \bmod n$, where $0 \leq \ell < n$. Then $\zeta^p = \zeta^\ell$, and a^p is in the ζ^ℓ-eigenspace of σ. Thus we can write $a^p = c_0 a^\ell + c_1 a^{\ell+n} + \cdots + c_m a^{\ell+mn}$ for $c_0, \dots, c_m \in K$.

An eigenbasis (i.e. a basis consisting of eigenvalues) is the union of bases for each eigenspace (since an eigenbasis exists if and only if the whole space is the direct sum of its eigenspaces).

Dividing both sides by a^ℓ gives a polynomial of a of degree $p - \ell$, so since a has degree p, we conclude that $\ell = 0$.

Therefore $p = 0 \bmod n$, so $n \mid p$, and so we must have $n = p$.

We claim that L is the splitting field of $x^p - a^p$.

First of all, we know that a^p has eigenvalue $\zeta^p = 1$, and so a^p is in the 1-eigenspace, which is K.

Our eigenbasis is $\{1, a, \dots, a^{p-1}\}$, and so the basis for the 1-eigenspace is $\{1\}$.

So $x^p - a^p \in K[x]$, and the roots are $a, \zeta a, \zeta^2 a, \dots, \zeta^p a$. Since $\zeta \in K$, the splitting field is $K(a) \subseteq L$. As we have shown, $K(a)/K$ has degree p, and so we must have $K(a) = L$.

3. Let k be a field of characteristic 0, and let L be an algebraic extension of k. For any $\alpha \in L$ we define a k-linear transformation $T_\alpha : L \to L$ by $T_\alpha(x) = \alpha \cdot x$. From this one obtains the Galois Norm $N_{L|k}$ defined by $N_{L|k}(\alpha) = \det(T_\alpha)$.

(a) Show if that if $\alpha \in k$, then $N_{L|k}(\alpha) = \alpha^n$ where $n = [L : k]$.

For $\alpha \in k$, $T_\alpha = \alpha I$, and $\det(\alpha I) = \alpha^{\dim_k L} = \alpha^{[L:k]}$

(b) Show that for any $\alpha, \beta \in L$ one has $N_{L|k}(\alpha\beta) = N_{L|k}(\alpha)N_{L|k}(\beta)$. Thus, $N_{L|K}$ is a homomorphism of groups $L^* \to k^*$. ← The groups of units.

$N_{L|k}(\alpha\beta) = \det(T_{\alpha\beta}) = \det(T_\alpha T_\beta) = \det(T_\alpha)\cdot\det(T_\beta) = N_{L|k}(\alpha)N_{L|k}(\beta)$.

(c) Show that if $L|k$ is a Galois extension, $N_{L|k}(x) = \prod_\sigma \sigma(x)$, where the product is over all elements of $Gal(L|k)$.

We will assume L/k is a finite extension.

$\sigma(\alpha) = \alpha$ for each $\sigma \in Gal(L/k)$, and $|Gal(L/k)| = [K:L]$ ↘ If $\alpha \in k$, then the claim follows from part a.

So assume $\alpha \notin k$, and consider the extension $k[\alpha] \subseteq L$. Let $m(x)$ be the minimal polynomial of α over k. Then T_α satisfies $m(x)$. Consider $T'_\alpha = T_\alpha|_{k[\alpha]}$.

$m(T_\alpha)y = m(\alpha)y = 0$. ← The characteristic polynomial of T'_α has degree $[k[\alpha]:k]$, which is the degree of $m(x)$, so it follows that $m(x)$ is the characteristic polynomial of T'_α, and the eigenvalues of T'_α are the roots of $m(x)$. Since L/k is Galois, these roots are distinct and contained in L. ← Normal: Irreducible $f \in k[x]$ with one root in L has all roots in L.

Note that even though $T_\alpha(y) = \alpha y$ for each $y \in L$, this does not mean that α is an eigenvalue for T_α, even if we extend $k \subseteq L$ and consider a vector space over L. This is because multiplication between elements in L will not have the same structure as scalar multiplication. For example, $\mathbb{R}(i) = \mathbb{R}^2$ as an $\mathbb{R}$-vector space, but multiplication by i in $\mathbb{R}(i) = \mathbb{C}$ is not the same as multiplying by the scalar i in the vector space $\mathbb{C}^2 \cong \mathbb{R}^2$

↑ Separable: the minimal polynomial over k of any $\alpha \in L$ is separable, i.e. has distinct roots

Theorem

Let F be a field, and let α be algebraic over F with minimal polynomial $f(x)$, and let $\varphi_0 : F \to \Omega$ be a homomorphism of F into a second field Ω. For every F-homomorphism $\varphi : F[\alpha] \to \Omega$, $\varphi(\alpha)$ is a root of $f(x)$ in Ω, and the map $\varphi \mapsto \varphi(\alpha)$ defines a 1-to-1 correspondence

$$\left\{\begin{matrix}F\text{-homomorphisms} \\ \varphi : F[\alpha] \to \Omega\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{roots of} \\ f \text{ in } \Omega\end{matrix}\right\}$$

or, more generally,

$$\left\{\begin{matrix}\text{extensions of } \varphi_0 \\ \varphi : F[\alpha] \to \Omega\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{roots of} \\ \varphi_0 f \text{ in } \Omega\end{matrix}\right\}$$

Now by the theorem, each of these roots is the image of α under a map $\tau : k[\alpha] \to L$ which fixes k, and such maps τ are in 1-to-1 correspondence with these roots, thus we can enumerate the roots $\{\tau(\alpha)\}$, and $\det T'_\alpha = \prod_\tau \tau(\alpha)$.

↑ product of eigenvalues.

Galois Extension Property

If E/F is Galois, and $E \subseteq K \subseteq F$, then a map $K \to F$ which fixes E can be extended to a map $F \to F$ in exactly $[F:K]$ ways.

The Galois extension property tells us that for each $\tau : k[\alpha] \to L$, there are exactly $[L : k[\alpha]]$ maps $\sigma \in Gal(L/k)$ with $\sigma(\alpha) = \tau(\alpha)$.

So $\prod_\sigma \sigma(\alpha) = \left(\prod_\tau \tau(\alpha)\right)^{[L:k[\alpha]]}$.

To finish the proof, we only need to show that $\det(T_\alpha) = \left(\det(T'_\alpha)\right)^{[L:k[\alpha]]}$. Let $n = [L : k[\alpha]]$, and let $\beta_1, \ldots, \beta_n$ be a basis of L as a vector space over $k[\alpha]$. Then T_α acts on $L/k[\alpha]$ as scalar multiplication, i.e. we can write the transformation as an $n \times n$ matrix αI_n. This matrix gives a $n \times n$ block diagonal matrix, which represents the transformation T_α on L/k. Each block corresponding to α is the matrix T'_α. Thus we get $\det(T_\alpha) = \det(T'_\alpha)^n$.

↑ Each b_i spans a copy of $k[\alpha]$, and the multiplication $\alpha\beta_i$ acts as T'_α on that copy of $k[\alpha]$.

If V is a vector space over k, and W is a vector space over V, then W is also a vector space over k. A transformation on $W/_V$ has a determinant, which is an element of V, say $\det T_v = d \in V$. Such a transformation is also on W/k, and has determinant $\det(T_k) = \det(d) \in k$, where d is now the transformation on W/k, defined by scalar multiplication by d on $W/_V$.

4. (January 2008 Problem 3) Working in the field of complex numbers, let ϵ be a primitive 16th root of unity, and let $\alpha = \epsilon\sqrt{2}$. Set $E = \mathbb{Q}[\epsilon]$, where $\mathbb{Q}$ is the field of rational numbers, let $f(X) = X^8 + 16 \in \mathbb{Q}[X]$, and note that α is a root of f(X).

(a) Show that $\sqrt{2} \in \mathbb{Q}[\epsilon^2]$.

ϵ^2 is a primitive 8^{th} root of unity, so $\mathbb{Q}[\epsilon^2]$ contains all primitive 8^{th} roots of unity. In particular $\beta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} \in \mathbb{Q}(\epsilon^2)$, and $\overline{\beta} = \cos\frac{\pi}{4} - i\sin\frac{\pi}{4} \in \mathbb{Q}(\epsilon^2)$, and we have $\sqrt{2} = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) + \left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = \beta + \overline{\beta} \in \mathbb{Q}(\epsilon^2)$.

(b) Conclude that $f(X)$ splits in E.

The roots of f(X) are $\epsilon\sqrt{2}, \epsilon^3\sqrt{2}, \epsilon^5\sqrt{2}, \ldots, \epsilon^{15}\sqrt{2}$, which we have shown are in E.

(c) If $G = Gal(E/\mathbb{Q})$, prove that no nonidentity element of G fixes α. Conclude that $f(X)$ is irreducible in $\mathbb{Q}[X]$.

The minimal polynomial of ϵ is the 8^{th} degree cyclotomic polynomial $\sum_{n=1}^{8} X^n$, which has primitive 16^{th} roots of unity as its roots. So the roots are $\{\epsilon^{2n+1}\}_{n=1}^{8}$. Any automorphism $\sigma \in Gal(E/\mathbb{Q})$ permutes these roots, and the permutation is uniquely defined by $\sigma(\epsilon)$.

So each $\sigma \in Gal(E/\mathbb{Q})$ has the form $\sigma(\epsilon) = \epsilon^{2n+1}$ for some $n \in \{0,1,\ldots,7\}$.
Since $\sqrt{2} = \epsilon^2 + \epsilon^{-2}$, we write $\alpha = \epsilon^3 + \epsilon^{-1}$. If σ fixes α, then we have $\epsilon^3 + \epsilon^{-1} = \epsilon^{6n+3} + \epsilon^{-2n-1}$.
Multiplying both sides by ϵ gives $\epsilon^4 + 1 = \epsilon^{6n+4} + \epsilon^{-2n}$. Noting that $\epsilon^4 = i$, we get

$$i + 1 = \epsilon^{6n+4} + \epsilon^{-2n}$$

Thus the σ which fix α correspond to the n such that $Re(\epsilon^{6n+4} + \epsilon^{-2n}) = Im(\epsilon^{6n+4} + \epsilon^{-2n}) = 1$.

Case 1: We eliminate the case $n = 1 \bmod 4$.
In this case, we have $4n = 4 \bmod 16$, and so

$$Re(\epsilon^{6n+4} + \epsilon^{-2n}) = Re(-\epsilon^{6n-4} + \epsilon^{-2n}) = Re(-\epsilon^{2n} + \epsilon^{-2n}) = 0.$$

($\epsilon^8 = -1$)

Case 2: We eliminate the case $n = -1 \bmod 4$.
In this case, we have $4n = -4 \bmod 16$, and so

$$Im(\epsilon^{6n+4} + \epsilon^{-2n}) = Im(\epsilon^{2n} + \epsilon^{-2n}) = 0$$

Case 3: We show that $n = 0$.
We know by the previous cases that n is even, so write $n = 2k$, where $k \in \{0,1,2,3\}$.
We have

$$i + 1 = \epsilon^{12k+4} + \epsilon^{-4k} = i\epsilon^{12k} + \epsilon^{12k} = \epsilon^{12k}(i+1) = (-i)^k(i+1)$$

Thus $(-i)^k = 1$, and so $k = 0$.

5. (August 2005 Problem 3) Let p and q be different prime numbers and consider the positive real numbers $\mu = \sqrt[p]{q}$ and $\nu = \sqrt[q]{p}$.

(a) Let F be a subfield of the real numbers $\mathbb{R}$ that does not contain μ. If $\mu^n \in F$ for some positive integer n, show that p divides n.

If $p \nmid n$, then we can find integers r_1, r_2 with $r_1 p + r_2 n = 1$. Then we have

$$\mu = \mu^{r_1 p + r_2 n} = (\mu^p)^{r_1} \cdot (\mu^n)^{r_2} = q^{r_1} (\mu^n)^{r_2} \in F, \quad \text{a contradiction.}$$

(b) Again, let $F \subseteq \mathbb{R}$ be a field not containing μ. Show that $[F[\mu] : F] = p$. (Hint: Consider the constant term of the minimal polynomial of μ over F.)

Since $\mu^p = q$, μ satisfies the polynomial $f(x) = x^p - q \in F[x]$. Thus we know $[F[\mu]:F] \leq p$. The roots of f are $\{\zeta^m \mu\}_{m=1}^{p-1}$, where ζ is a primitive p^{th}-root of unity. If $g(x)$ is the minimal polynomial of μ, then the roots of g are a subset of these roots. The constant term of g will be the product of its roots, and so we have $g(0) = \prod_{j=1}^{d} \zeta^{m_j} \mu$, where $d = \deg(g)$. If $m = \sum_{j=1}^{d} m_j$, then we have $g(0) = \zeta^m \mu^d \in F$. Since $F \subseteq \mathbb{R}$, we must have $\zeta^m = \pm 1$, and in either case, $\mu^d \in F$, and so we conclude that $p \mid d$. Since $d = [F[\mu]:F] \leq p$, we see that $[F[\mu]:F] = p$.

(c) Now let $F = \mathbb{Q}[\mu + \nu]$ be the field extension of the rationals $\mathbb{Q}$ generated by $\mu + \nu$. Show that $[F : \mathbb{Q}] = pq$.

$[\mathbb{Q}[\mu,\nu]:\mathbb{Q}[\mu]] = q$, $[\mathbb{Q}[\mu]:\mathbb{Q}] = p$

We claim that $F = \mathbb{Q}[\mu,\nu]$. Note that part b implies $[\mathbb{Q}[\mu,\nu]:\mathbb{Q}] = pq$.
Clearly $F \subseteq \mathbb{Q}[\mu,\nu]$. Also note that $F[\mu] = F[\nu] = \mathbb{Q}[\mu,\nu]$ ($\nu = (\mu+\nu) - \mu \in F[\mu]$)
If $F \neq \mathbb{Q}[\mu,\nu]$, then F does not contain either μ or ν.
In this case, part b implies $[F[\mu]:F] = p$, $[F[\nu]:F] = q$, which is a contradiction.

1. (January 2013 Problem 2) Let k be a field. We say a polynomial in $k[x]$ is a *consecutive-root polynomial* if it has two roots x_0, x_1 (not necessarily in k) which satisfy $x_1 - x_0 = 1$.

(a) Show that there is no irreducible consecutive-root polynomial in $\mathbb{Q}[x]$.

Suppose $f \in \mathbb{Q}[x]$ is irreducible and consecutive root, with $f(\alpha) = f(\alpha+1) = 0$ for $\alpha \in \mathbb{C}$. Let K be the splitting field for $f(x)$ over $\mathbb{Q}$. Then $K/\mathbb{Q}$ is a Galois extension, and so there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) = \alpha + 1$. Then $\sigma^n(\alpha) = \alpha + n \neq \alpha$, which implies σ has infinite order. This is a contradiction, since $K/\mathbb{Q}$ is a finite extension.

A finite extension E/F is Galois if and only if E is a splitting field of a separable polynomial in $F[x]$.

(b) Let p be a prime number. Show that the polynomial $x^p - x - 1$ in $\mathbb{F}_p[x]$ is irreducible and consecutive root.

If α is a root of $f(x) = x^p - x - 1$, then $f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - 1 = \alpha^p + 1 - \alpha - 2 = f(\alpha) = 0$. This shows that f is consecutive root, and that the roots are $\{\alpha + n\}_{n=0}^{p-1}$.

Fermat's Little Theorem
If p is prime, and a is any integer, then $a^p \equiv a \bmod p$.

Note that Fermat's Little Theorem implies $\alpha \notin \mathbb{F}_p$, since $f(a) = a^p - a - 1 = -1$ for any $a \in \mathbb{F}_p$.

Now we want to show that f is irreducible. If $g \mid f$, then the roots of g are some subset of the roots of the roots of f, say $\{\alpha + n_i\}_{i=1}^{d}$, where $d = \deg(g)$. If $g(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then we know $\pm a_{d-1}$ is the sum of the roots of g. So we know $\sum_{i=1}^{d} \alpha + n_i = \pm a_{d-1} \in \mathbb{F}_p$. This implies that $d\alpha \in \mathbb{F}_p$. If $d < p$, then d has an inverse $d^{-1} \in \mathbb{F}_p$, and so we conclude that $\alpha \in \mathbb{F}_p$, a contradiction. It follows that $g = f$, and so f must be irreducible.

(c) Describe the set of irreducible monic consecutive-root polynomials in $\mathbb{F}_p[x]$ of degree at most p.

Note that the reasoning in part b also applies to $f(x) = x^p - x - k$ for any integer k. We claim that all irreducible monic consecutive root polynomials in $\mathbb{F}_p[x]$ have this form.

To construct a finite field of order p^n, choose any irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n. $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f(x))$ is a field of order p^n.

The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is always Galois.

Let f be an irreducible consecutive-root polynomial in $\mathbb{F}_p$ and let $n = \deg(f) \geq p$. The splitting field of $f(x)$ over $\mathbb{F}_p$ is $\mathbb{F}_p[x]/(f(x)) = \mathbb{F}_{p^n}$, and the extension is Galois.

Now if $\alpha, \alpha+1$ are roots of f, then there is an automorphism $\sigma : \alpha \mapsto \alpha + 1$. Since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$ is cyclic of order n, we must have $\sigma^n = \mathrm{id}$. This implies that $\sigma^n(\alpha) = \alpha + n = \alpha$, and so $p \mid n$, which implies $n = p$.

This means σ generates $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$, and so we must have $\sigma^k : x \mapsto x^p$ be the Frobenius map for some k. Then $\alpha^p = \sigma^k(\alpha) = \alpha + k$, and so α satisfies $x^p - x - k$. Since $f(x)$ has degree p, we conclude that $f(x) = x^p - x - k$.

Frobenius Automorphism
In $\mathbb{F}_{p^n}$, the map $\varphi : x \mapsto x^p$ is a $\mathbb{F}_p$-linear endomorphism, and an automorphism of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, and is generated by the Frobenius map.

2. (January 2014 Problem 5) If L/K is a field extension, we say a field K' is *intermediate* between L and K if it properly contains K and is properly contained in L.

   (a) Prove that a *separable* field extension L/K of degree 4 has at most 3 intermediate fields. Give an example of a field extension L/K of degree 4 which has exactly 3 intermediate fields.

Let L/K be a separable degree 4 extension. If L/K has at most 1 intermediate field, we are done, so assume L_1, L_2 are distinct intermediate fields. Clearly L_1/K and L_2/K must be degree 2, and so $L_1 = K(\alpha)$, $L_2 = K(\beta)$, where α and β have degree 2 minimal polynomials $f, g \in K[x]$, respectively. Since $\alpha, \beta \in L$ and L/K is separable, it follows that $f(x)$ and $g(x)$ are separable.

A separable extension is an algebraic extension $E \supset F$ such that for every $\alpha \in E$, the minimal polynomial of α over F is separable.

We claim that L is the splitting field of $f(x)g(x)$, which implies L/K is Galois. Since $K(\alpha)$, $K(\beta)$ are degree 2 extensions, they must be normal extensions, and so $f(x)$ splits in $K(\alpha)$, and $g(x)$ splits in $K(\beta)$.

Every degree 2 extension is normal. In characteristic $\neq 2$ it is also separable and therefore Galois.

This means $f(x)g(x)$ splits in L. Now the splitting field of $f(x)g(x)$ must contain $K(\alpha, \beta)$, a degree 4 extension, and so we must have $K(\alpha, \beta) = L$ is the splitting field of $f(x)g(x)$. Since $g(x)f(x)$ is separable, we conclude that L/K is Galois.

Thus L/K has Galois group G of order 4, and the intermediate fields of L/K are in 1-to-1 correspondence with the subgroups of G. The only groups of order 4 are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which have 1 subgroup, and 3 subgroups, respectively.

We could also use the fact that L_1/K, L_2/K Galois $\Rightarrow L_1L_2/K$ Galois, and note $K(\alpha)K(\beta) = K(\alpha, \beta) = L$.

Our analysis shows that $K[\alpha, \beta]/K$ will always have 3 intermediate fields when this extension is separable and $K[\alpha] \neq K[\beta]$ are degree 2 extensions. In particular, we could take $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$.

(b) Give an example of a field extension L/K of degree 4 such that there is no intermediate field K' between L and K.

Our analysis in part a shows that this cannot be the case if L/K is Galois. However, suppose F/K is Galois, with $G = \mathrm{Gal}(F/K)$. Then if H is an index 4 subgroup of G which is not properly contained in any other subgroup of G, we know H corresponds to a subfield L of F with the desired properties.

$[G:H] = [L:K]$, and intermediate fields of L/K correspond with subgroups of G containing H.

Let $G = A_4$, the Alternating group on 4 elements. $|A_4| = 12$, and is generated by 3-cycles. A_n is generated by 3-cycles for any n.

A_4 certainly has index 4 subgroups, since 3-cycles have order 3. However, there is no subgroup of order 6, since adding any 3-cycle as a generator to a subgroup of order 3 spans all of A_4.

e.g. $\langle (123), (23,4) \rangle = A_4$
$(123)(243) = (412)$
$(132)(234) = (413)$ →

So we need to construct a field extension F/E which has Galois group A_4.

To construct any finite Galois group:
Let G be a finite group. Then G inbeds into S_n.
Let K be any field. Let $F = K(x_1, \ldots, x_n)$. $L = K(e_1, \ldots, e_n)$, $e_j = \sum_{i_1 < \cdots < i_j} \prod x_{i_j}$.
Then $\mathrm{Gal}(F/L) = S_n$. Define E to be the fixed field of the subgroup $G \leq \mathrm{Gal}(F/L)$.
Then $\mathrm{Gal}(F/E) = G$.

3. (August 2011 Problem 3) Let $K \subseteq F \subseteq E$ be fields with $E = F[\alpha]$ and with $\alpha^n \in F$ for some positive integer n. Suppose K contains a primitive nth root of unity, and let L be a field with $K \subseteq L \subseteq E$ and $L \cap F = K$.

(a) If L is Galois over K, show that $L = K[\beta]$ for some element β with $\beta^n \in K$.

If $n|m$, then $\beta^n \in K \Rightarrow \beta^m \in K$, and ζ primitive m^{th} root of unity $\Rightarrow \zeta^{m/n}$ is a primitive n^{th} root of unity.

Without loss of generality, we can assume n is the smallest positive integer with $\alpha^n \in F$

The only inseparable irreducible polynomials are of the form $f(x^p)$ in characteristic p.

If $\operatorname{char} F = 0$, then every irreducible $f \in F[x]$ is separable.

The minimal polynomial of α divides $x^n - \alpha^n$, and is thus separable if $\operatorname{char} K \nmid n$.

The term "primitive n^{th} root of unity" implies that $\operatorname{char} F$ does not divide n, which implies $F[\alpha]/F$ is separable.

Let $\zeta \in K$ be a primitive n^{th} root of unity. Then the roots of $x^n - \alpha^n$ are $\{\zeta^j \alpha\}_{j=0}^{n-1}$. These roots are all contained in $F[\alpha]$, but in no proper subfield, and so $F[\alpha]$ must be the splitting field of $x^n - \alpha^n$ over F. We conclude that $F[\alpha]/F$ is Galois.

Since $\zeta \in K$, we see that an automorphism $\sigma \in \operatorname{Gal}(F[\alpha]/F)$ is uniquely determined by the choice $\sigma(\alpha) = \zeta^j \alpha$ for $j \in \{1, \dots, n\}$, and since $\sigma^m(\alpha) = \zeta^{jm}\alpha$, we conclude $\operatorname{Gal}(F[\alpha]/F) = \mathbb{Z}/n\mathbb{Z}$.

Since $\mathbb{Z}/n\mathbb{Z}$ is abelian, every subgroup is normal, and so any intermediate field of $F[\alpha]/F$ is Galois over F. In particular, since $F \subseteq FL \subseteq F[\alpha]$, we have FL/F is Galois with Galois group which is a quotient of $\mathbb{Z}/n\mathbb{Z}$. So we have $\operatorname{Gal}(FL/F) = \mathbb{Z}/m\mathbb{Z}$ for some $m|n$.

Normal subgroups correspond to Galois extensions over the base field.

All intermediate fields of a separable extension are separable, and normal subgroups correspond to normal extensions.

For Galois extensions $K \subseteq F \subseteq E$, $\operatorname{Gal}(F/K) = \operatorname{Gal}(E/K)/\operatorname{Gal}(E/F)$

Define $\psi : \operatorname{Gal}(L/K) \to \operatorname{Gal}(FL/F)$, $\sigma \mapsto \sigma'$, where $\sigma'|_L = \sigma$, and $\sigma'|_F = \mathrm{id}$.

Note that this makes sense since $\sigma = \mathrm{id}$ on $L \cap F = K$. Now $\psi(\sigma) = \sigma' = \mathrm{id}$ implies $\sigma'|_L = \mathrm{id}$, i.e. $\sigma = \mathrm{id}$. Thus ψ is injective, and so $\operatorname{Gal}(L/K)$ is a subgroup of $\mathbb{Z}/m\mathbb{Z}$, say $\mathbb{Z}/m'\mathbb{Z}$. So L/K is a cyclic extension, i.e. $L = k[\beta]$ for some $\beta^{m'} \in K$. Since $m'|m|n$, we are done.

4. (January 1994 Problem 3) Let α be the real positive 16th root of 3 and consider the field $F = \mathbb{Q}[\alpha]$ generated by α over the rationals $\mathbb{Q}$. Notice that we have the chain of intermediate fields

$$\mathbb{Q} \subseteq \mathbb{Q}[\alpha^8] \subseteq \mathbb{Q}[\alpha^4] \subseteq \mathbb{Q}[\alpha^2] \subseteq \mathbb{Q}[\alpha] = F$$

(a) Compute the degrees of these five intermediate fields over $\mathbb{Q}$ and conclude that these fields are all distinct.

$\alpha^8 = \sqrt{3}$, $\alpha^4 = \sqrt[4]{3}$, $\alpha^2 = \sqrt[8]{3}$, and $\alpha = \sqrt[16]{3}$ have minimal polynomials x^2-3, x^4-3, x^8-3, and $x^{16}-3$ over $\mathbb{Q}$, respectively. Thus the degrees over $\mathbb{Q}$ are $2, 4, 8, 16$.

(b) Show that every intermediate field between $\mathbb{Q}$ and F is one of the above. (Hint: If $\mathbb{Q} \subseteq K \subseteq F$, consider the constant term of the minimal polynomial α over K.)

Since $[F:\mathbb{Q}] = 16$, we must have $[F:K][K:\mathbb{Q}] = 16$. Let $f(x)$ be the minimal polynomial of α over K. Then since $F = K(\alpha)$, the degree of f is $[K:\mathbb{Q}]$, and thus divides 16. We also know $f(x)$ divides $x^{16} - 3$.

Now the roots of $f(x)$ are roots of $x^{16}-3$, so they have the form $\zeta^{n_i}\alpha$ for $i = 1, \ldots, \deg(f)$. The constant term $f(0) = \prod_i \zeta^{n_i}\alpha$ is an element of $K \subseteq F$, and is therefore real.

We conclude that $\prod_i \zeta^{n_i} = \zeta^{\sum_i n_i}$ is real, and so $\sum_i n_i = 8$ or 16.

In particular, $f(0) = \pm\alpha^n$, so $\alpha^n \in K$, where $n = \deg(f)$, and so $\mathbb{Q}(\alpha^n) \subseteq K$. Now $[K:\mathbb{Q}] = \frac{16}{n} = [\mathbb{Q}(\alpha^n):\mathbb{Q}]$, so it follows that $K = \mathbb{Q}(\alpha^n)$.