Question #2

Determine the group of field automorphisms of GF(4).

$GF(4) := (\mathbb{Z}/2)[X]/\langle X^2+X+1\rangle$ a field with 4 elements

$X^2+X+1=0$

$\therefore X^2+X=-1=1$ in $\mathbb{Z}_2$

the 4 elements are $\{0, 1, X, 1+X\}$

φ: $0 \to 0$, $1 \to 1$, $a \to a$, $1+a \to 1+a$

φ: $0 \to 0$, $1 \to 1$, $a \to 1+a$, $1+a \to a$

The two field automorphisms of GF(4) group

2/2

Question #4

Given that the automorphism group of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ is isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$, determine the number of subfields of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ that have degree 4 over $\mathbb{Q}$.

The number of subfields with degree 4 over $\mathbb{Q}$ is the same as the number of subgroups of $Z_2 \oplus Z_2 \oplus Z_2$ with order 2. Since every element of $Z_2 \oplus Z_2 \oplus Z_2$ other than the identity has order 2, there are 7 elements of order 2, which means 7 subgroups of order 2, which means that there are 7 subfields of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ of degree 4 over $\mathbb{Q}$.

Question #6.

Let E be the splitting field of X^4+1 over $\mathbb{Q}$. Find $Gal(E/\mathbb{Q})$. Find all subfields of E. Find the automorphisms of E. That have fixed fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(i)$. Is there an automorphism of E whose fixed field of $\mathbb{Q}$?

Use the DeMoivre's Theorem, find the roots of X^4+1, write $X^4 = -1 = e^{\pi i}$, so the roots are $\zeta = e^{\pi/4}$, ζ^3, ζ^5, and ζ^7. The galois group consists of 4 elements:

$\sigma_1(\zeta) = \zeta$
$\sigma_3(\zeta) = \zeta^3$
$\sigma_5(\zeta) = \zeta^5$
$\sigma_7(\zeta) = \zeta^7$

21/2

Because $\zeta^8 = 1$, a simple computation shows that each of these 4 automorphisms has order 2, and therefore the Galois group is isomorphic to $Z_2 \oplus Z_2$ ✓

One subgroup of the Galois group is $\{\sigma_1, \sigma_3\}$. It has fixed field $\mathbb{Q}(\zeta+\zeta^3)$, because $\sigma_3(\zeta+\zeta^3) = \zeta^3+\zeta^9 = \zeta^3+\zeta$. Use trigonometry to identify this field: $\zeta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}+i\sqrt{2}}{2}$ and $\zeta^3 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = \frac{-\sqrt{2}+i\sqrt{2}}{2}$. Therefore $\zeta+\zeta^3 = i\sqrt{2}$, so $\mathbb{Q}(\zeta+\zeta^3) = \mathbb{Q}(i\sqrt{2}) = \mathbb{Q}(\sqrt{-2})$.

Another subgroup of the Galois group is $\{\sigma_1, \sigma_5\}$. We could imitate what we did above, and say that this subgroup has fixed field $\mathbb{Q}(\zeta+\zeta^5)$, because $\sigma_5(\zeta+\zeta^5) = \zeta^5+\zeta^{25} = \zeta^5+\zeta$. Use trigonometry to identify this field: $\zeta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}+i\sqrt{2}}{2}$ and $\zeta^5 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = \frac{-\sqrt{2}-i\sqrt{2}}{2}$. Therefore $\zeta+\zeta^5 = 0$, so we have not found anything at all

Alternatively, we can note that this subgroup fixes ζ^2,

because $\sigma_5(\zeta^2) = \sigma_5(\zeta)^2 = \zeta^{10} = \zeta^2$. We can also compute that $\zeta^2 = e^{\pi i/2} = i$, so this fixed field is $\mathbb{Q}(i)$.

The third subgroup of the Galois group is $\{\sigma_1, \sigma_7\}$. It has fixed field $\mathbb{Q}(\zeta + \zeta^7)$, because $\sigma_7(\zeta + \zeta^7) = \zeta^7 + \zeta^{49} = \zeta^7 + \zeta$. We can use trigonometry to identify this field:

$\zeta = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + \frac{i\sqrt{2}}{2}$ and $\zeta^7 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{\sqrt{2} - i\sqrt{2}}{2}$

Therefore $\zeta + \zeta^7 = \sqrt{2}$, so $\mathbb{Q}(\zeta + \zeta^7) = \mathbb{Q}(\sqrt{2})$.

There is no automorphism of E with fixed field $\mathbb{Q}$, because such an automorphism would have to have order 4.

Question #8

Show that the Galois group of a polynomial of degree n has order dividing n!

Define: $\varphi \longrightarrow S_n$

$\sigma \longrightarrow \sigma$ permutes all rest of f.

φ injective $\quad \sigma|_F = id \quad$ n elements.

$\sigma \to \sigma$ is identity

$\therefore \ker \sigma$ is identity

if $\sigma \in S_n$ is identity then σ fixed all root

$\therefore \sigma$ fixed all field

$\therefore \sigma$ must be identity

$\#\varphi(G) = \#(G)$ $\therefore$ carnality same because φ injective

$\therefore \varphi(G) < S_n$

$\varphi(G)$ is a subgroup of S_n

$\therefore \#\varphi(G) \mid \#S_n$ by the lagrange thm

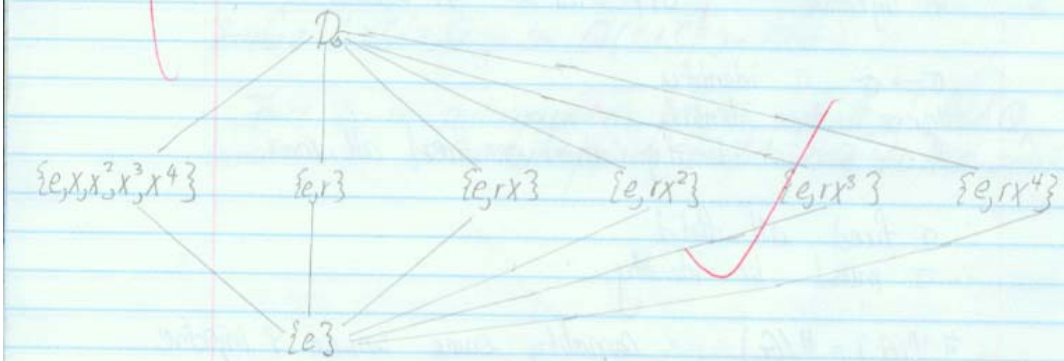
$\#S_n = n!$

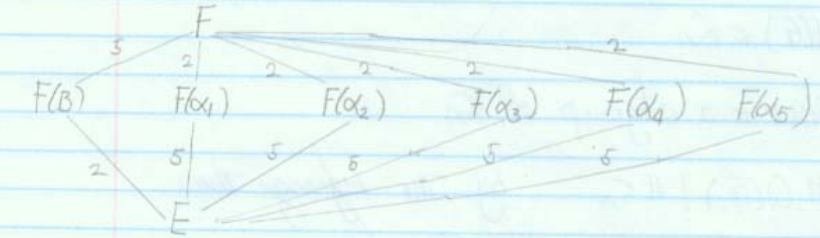
$\therefore$ The galois group of a polynomial of degree n has order dividing n!

Question 14

Suppose that E is the splitting field of some polynomial over a field F of characteristic 0. If $Gal(E/F)$ is isomorphic to D_5, draw the subfield lattice for the fields between E and F.

$D_5 = \{e, x, x^2, x^3, x^4, r, rx, rx^2, rx^3, rx^4\}$.





if element of form x^j assume j is 0, 1, 2, 3, 4 then H is in subgroup $\{e, x, x^2, x^3, x^4\}$

otherwise, for the element of the form rx^k. $k = 0, 1, 2, 3, 4$. H is in one of those 5 subgroups.

any two element from D_5 will generate the whole group unless they are both x.

Proof:

$(rx^j)(x^k)^{-1}$
$= rx^{j+k}$
$= r$

$(rx^j)(rx^k)$
$= r(x^j r)x^k$
$= r(rx^{-j})x^k = x^{kj}$

Question 15

Suppose that $F \subset K \subset E$ are fields and E is the splitting field of some polynomial in $F[x]$. Show, by means of an example, that K need not be the splitting field of some polynomial in $F[x]$.

Let w be a primitive cube root of 1. Then $Q \subset Q(\sqrt[3]{2}) \subset Q(w, \sqrt[3]{2})$ and $Q(\sqrt[3]{2})$ is not the splitting field of a polynomial in $Q[x]$.

4/4