#2. c. Find basis and degree of $\mathbb{Q}(\sqrt{2}, i)$

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$: min poly. $x^2 - 2 \in \mathbb{Q}[x]$

$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]$: has min poly $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$

$$\therefore [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$$

basis $= \{1, \sqrt{2}, i, \sqrt{2}i\}$

#3) b) Find Splitting field of $x^4 + 1$

The 4 roots of $x^4 + 1$ over $\mathbb{C}$ are $x = \pm 1 \pm i$

Let E = Splitting field of $x^4 + 1$

All roots are in $\mathbb{Q}(i)$ $\therefore$ $E \subseteq \mathbb{Q}(i)$

but $\mathbb{Q}(i)$ has $\mathbb{Q}$-basis $\{1, i\}$

and we cannot express all roots of $x^4 + 1$

with any proper subset of this basis

$\therefore$ $E = \mathbb{Q}(i)$.

14.) **14.** Let K be an algebraic extension of E, and E an algebraic extension of F. Prove that K is algebraic over F. [*Caution*: Do not assume that the extensions are finite.]

Proof:

Want to show K is alg. over F.

Let $\alpha \in K$ and let

$$p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$$ be the

minimal polynomial of α over E, (so $p(x) \in E[x]$)

$b_0, \ldots, b_{n-1} \in E$ are algebraic over F since E is an algebraic extension of F. Note that $p(x) \in F(b_0, \ldots, b_{n-1})[x]$.

Since $F(b_0, \ldots, b_{n-1}) \subset E$ $\therefore$ α is a root of

$p(x) \in F(b_0, \ldots, b_{n-1})[x]$.

$\therefore$ α is algebraic over $F(b_0, \ldots, b_{n-1})$.

But this means α is algebric over F since each

b_j is algebraic over F and there are finitely many

b_j. ∎

#26) **26.** Let α, β be transcendental over $\mathbb{Q}$. Prove that either $\alpha\beta$ or $\alpha+\beta$ is also transcendental.

Suppose $\alpha\beta$ and $\alpha+\beta$ are algebraic, let

$E = \overline{\mathbb{Q}}$ denote the field of algebraic numbers,

that is the algebraic closure of $\mathbb{Q}$.

then $\alpha\beta$; $\alpha+\beta \in E$

$\therefore$ $x^2 - (\alpha+\beta)x + \alpha\beta \in E[x]$

But then $x^2 - (\alpha+\beta)x + \alpha\beta = (x-\alpha)(x-\beta) \in E[x]$

$\Rightarrow \alpha, \beta \in E \Rightarrow \alpha$ and β are algebraic numbers

This is a contradiction

$\therefore$ either $\alpha\beta$ is transcendental

or $\alpha+\beta$ is transcendental (or both). ∎

Section 22.3:

#12: Prove or disprove: There exists a finite field that is algebraically closed.

A finite field cannot be algebraically closed.

Proof: Let F be a finite field with elements

$a_1, \cdots, a_n$, Since F is a field $\Rightarrow 1 \in F \therefore a_j = 1$ for some j.

Then $f(x) = (x-a_1)\cdots(x-a_n) + 1 \in F[x]$

Since $a_1, \cdots, a_n \in F$ and $1 \in F$.

But $f(a_j) = 1 \quad \forall j = 1, \cdots, n$

$\therefore$ $f(x) \in F[x]$ has no roots in F since $a_1, \cdots, a_n$ are all elements of F.

Since there exists a polynomial with no roots

in F then F cannot be algebraically closed.

∎

20)

20. Show that for every n there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.

Proof: For every n $\exists$ a finite field isomorphic to $GF(p^n)$ containing p^n elements.

we know $GF(p^n)$ must be a simple extension of $\mathbb{Z}_p$

so $GF(p^n) = \mathbb{Z}_p(\alpha)$ for some $\alpha \in GF(p^n)$

and since $|GF(p^n)| = p^n$ and $|\mathbb{Z}_p| = p$ (specifically the generator of $(GF(p^n))^*$)

$\Rightarrow$ any $\mathbb{Z}_p$-basis for $GF(p^n)$ contains n elements i.e. $\{1, \alpha, \dots, \alpha^n\}$

(otherwise $GF(p^n)$ would not contain p^n elements)

$\therefore$ $[GF(p^n) : \mathbb{Z}_p] = n$

Let $p(x)$ be the minimal polynomial of α, then $p(x) \in \mathbb{Z}_p[x]$, $\deg(p(x)) = n$ and $p(x)$ is irreducible since it is a minimal polynomial. ∎

21)

21. Prove that the ***Frobenius map*** $\Phi : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ given by $\Phi : \alpha \mapsto \alpha^p$ is an automorphism of order n.

Proof: $GF(p^n)$ is a field and $\mathrm{char}(GF(p^n)) = p$,

Let $\alpha, \beta \in GF(p^n)$

$\Phi(\alpha \cdot \beta) = (\alpha\beta)^p \overset{\text{since mult. is comutative}}{=} \alpha^p \beta^p$

$\Phi(\alpha + \beta) = (\alpha + \beta)^p \overset{\text{see the proof of lemma 22.3 of our Book, follows from the binomial formula since all other terms will be multiplied by } p.}{=} \alpha^p + \beta^p$

$\therefore$ Φ is a homomorphism from $GF(p^n)$ to itself

show 1-1 and onto:

If $\Phi(\alpha) = \alpha^p = 0$, then since $GF(p^n)$ is a field

it cannot contain zero divisors

$\therefore$ $\alpha = 0$ $\therefore$ Φ is 1-1.

But a 1-1 map between finite sets must be onto

$\therefore$ Φ is an auto morphism.

I don't think that we defined the order of an automorphism in class... so you wouldn't be expected to know that

it wants you to then show that

$\Phi^{(n)} = \Phi \circ \cdots \circ \Phi$ = identity map.

(n-times)

Suppose $\beta \neq 0$

$\Phi^{(n)}(\beta) = \beta^{p^n}$, $|GF(p^n)^*| = p^n - 1$ (group of units)

and $\beta \in GF(p^n)^*$

$\therefore$ by Lagranges theorem $\beta^{p^n - 1} = 1$ (any element to the order of the group must be the groups identity, in this case 1)

$\therefore$ $\beta^{p^n} = \beta$ $\forall \beta \neq 0$ and also true if $\beta = 0$

$\therefore$ $\Phi^{(n)}$ = identity.

■

#22

22. Show that every element in $\mathrm{GF}(p^n)$ can be written in the form a^p for some unique $a \in \mathrm{GF}(p^n)$.

Proof:

The Frobenius map $\Phi : a \mapsto a^p$ is an automorphism $\therefore$ for every $b \in GF(p^n)$ $\exists$ a unique element $b = \Phi(b) = b^p$, that is all elements must be the result of applying the Frobenius automorphism to some unique element. ∎