3/4
Weds
week 7

Ex: $V = \mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$

$F = \mathbb{C}$

basis for $V=\mathbb{C}$ over $F=\mathbb{C}$ is $\beta = \{1\}$

span: $\text{span}\{1\} = \{\alpha \cdot 1 \mid \alpha \in \mathbb{C}\} = \mathbb{C}$

lin. ind.: If $\alpha \cdot 1 = 0$, then $\alpha = 0$.

The
b
t

Def
If
of
dime

$\{1\}$

Theorem: If $\{a_1, a_2, \dots, a_n\}$ and $\{b_1, b_2, \dots, b_m\}$ are both bases for a vector space V over a field F, then $n = m$.

Def: Let V be a vector space over a field F. If there exists a finite basis for V over F of size n, then we say that V has dimension n over F and write $\dim_F(V) = n$.

Ex:

$\dim_{\mathbb{R}}(\mathbb{C}) = 2 \leftarrow$ basis $\{1, i\}$

$\dim_{\mathbb{C}}(\mathbb{C}) = 1 \leftarrow$ basis $\{1\}$

Chapter 13

13.1 – Basic theory of field extensions

Def: Let F be a field and 1 be its multiplicative identity. The characteristic of F, denoted $ch(F)$, is defined to be the smallest positive integer p such that

$$\underbrace{p \cdot 1}_{\text{notation}} = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0$$

0.

if such a p exists.
If no such p exists
then we say F has
characteristic 0.

Ex:

$ch(\mathbb{Z}_p) = p$

$ch(\mathbb{Q}) = 0$

$ch(\mathbb{R}) = 0$

$ch(\mathbb{C}) = 0$

Prop: Let F be a field.
Then either $ch(F) = 0$
or $ch(F) = p$ where p is prime.
If $ch(F) = p$, then

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0$$

for all $\alpha \in F$.

$\boxed{\text{PROOF}}$: If $ch(F)=0$, then we're done.

Let $ch(F)=p$ where p is a positive integer.

Suppose p is not prime.

Then $p=ab$ where $1<a<p$ and $1<b<p$.

It follows that

$$0 = \underbrace{p\cdot 1}_{\substack{1+1+\cdots+1 \\ p \text{ times}}} = \underbrace{(a\cdot 1)}_{\substack{1+1+\cdots+1 \\ a \text{ times}}}\underbrace{(b\cdot 1)}_{\substack{1+1+\cdots+1 \\ b \text{ times}}}$$

So either $a\cdot 1=0$ or $b\cdot 1=0$.

But p is the smallest positive integer where $p\cdot 1=0$.

So we can't have

$a\cdot 1=0$ and $1<a<p$

or $b\cdot 1=0$ and $1<b<p$.

So, p must be prime.

smallest
where $p\cdot 1 = 0$.

e

$1 < a < p$

$1 < b < p$.

prime,

Let $\alpha \in F$.

Then

$$
\begin{aligned}
p\cdot\alpha &= p\cdot(1\alpha) \\
&= \underbrace{1\alpha + 1\alpha + \cdots + 1\alpha}_{p \text{ times}} \\
&= \underbrace{(1+1+\cdots+1)}_{p \text{ times}}\alpha = (p\cdot 1)\alpha \\
&= 0\alpha \\
&= 0.
\end{aligned}
$$

$\blacksquare$

Def: The <u>prime subfield</u> of a field F is the smallest subfield of F that contains 1.

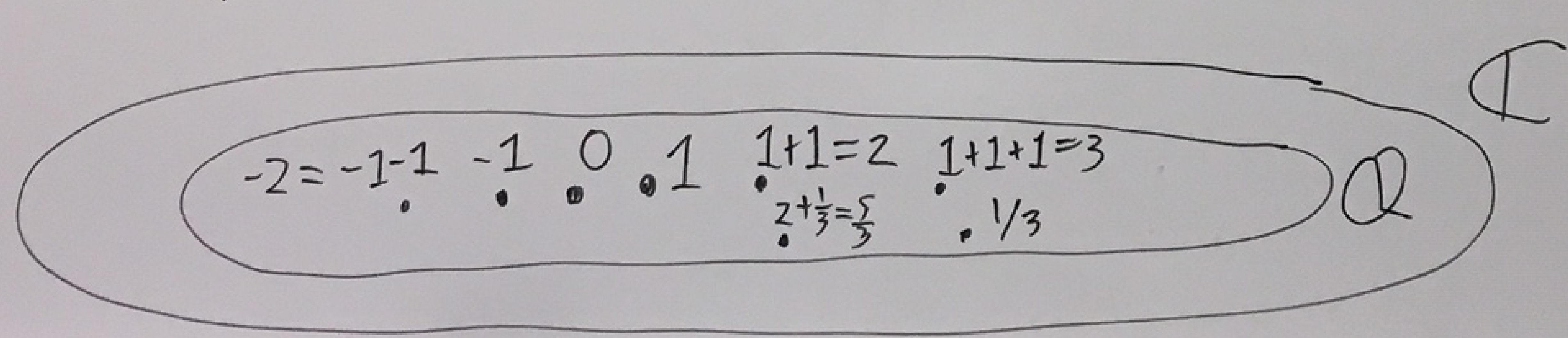
[Its also the subfield that is generated by 1]

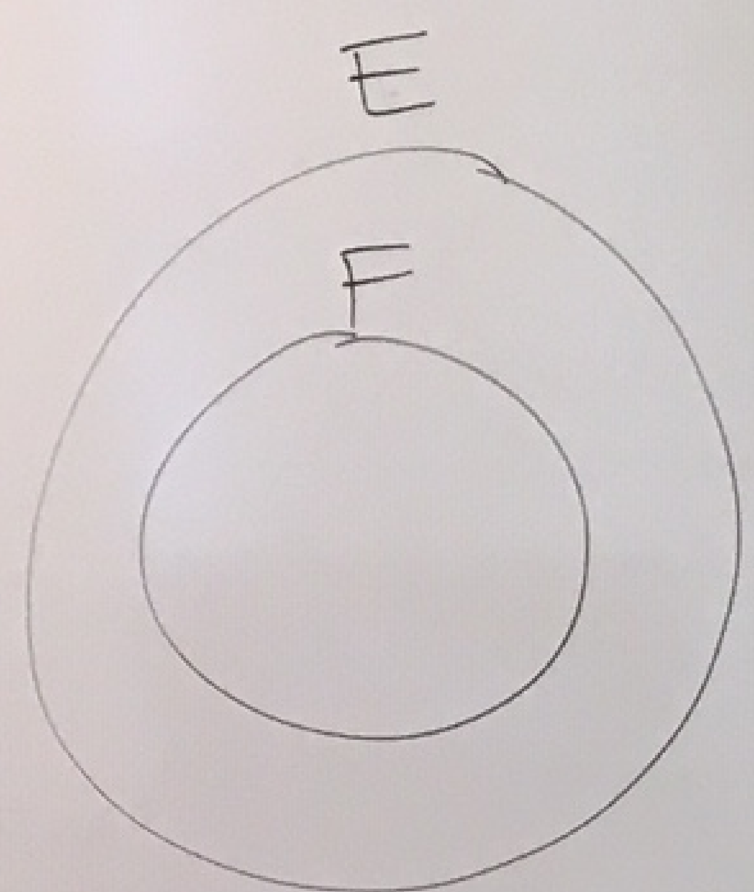
Facts:

If $ch(F)=0$, then its prime subfield is isomorphic to $\mathbb{Q}$.

If $ch(F)=p$, then its prime subfield is isomorphic to $\mathbb{Z}_p$.

Ex: prime subfield of $\mathbb{C}$ is $\mathbb{Q}$





Def: If E is a field and F is a subfield of E, then we call E an <u>extension field</u> of F. We write E/F to mean that E is an extension field of F. Or we use the diagram

$$\begin{array}{c} E \\ | \\ F \end{array}$$

Def: If E is an extension field of F, then we can think of E as a vector space over F. Here E is V and scalar multiplication

$$\alpha v$$

where $\alpha \in F$ and $v \in E$ is the field multiplication.

F,

or

ation

$v \in E$

plication.

The <u>degree</u> of the field extension E/F, denoted by $[E:F]$, is the dimension of the vector space E over the field F.

That is, $[E:F] = \dim_F(E)$.

We call E/F a <u>finite extension</u> if $[E:F]$ is finite.

<u>Ex</u>: $\mathbb{C}$ is an extension field of $\mathbb{R}$.

A basis for $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$.

So, $[\mathbb{C}:\mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = 2$

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash, "2"] \\ \mathbb{R} \end{tikzcd}$$

Theorem: Let F be a field and let $p(x) \in F[x]$.
where $p(x)$ is an irreducible, non-constant polynomial.
Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root.
Identifying F with this isomorphic copy shows that there exists an extension of F where $p(x)$ has a root.

Ex: $F = \mathbb{R}$, $p(x) = x^2+1$

p has no roots in $\mathbb{R}$
and has degree 2
so $p(x)$ is irreducible over $\mathbb{R}$

Since $p(x)$ is irreducible in $\mathbb{R}[x]$,
the ideal $I = (x^2+1) = \{(x^2+1)f(x) \mid f(x) \in \mathbb{R}[x]\}$ is maximal
and $K = \mathbb{R}[x]/I = \mathbb{R}[x]/(x^2+1)$ is a field.

Claim: $K = \{(a+bx)+I \mid a,b \in \mathbb{R}\}$

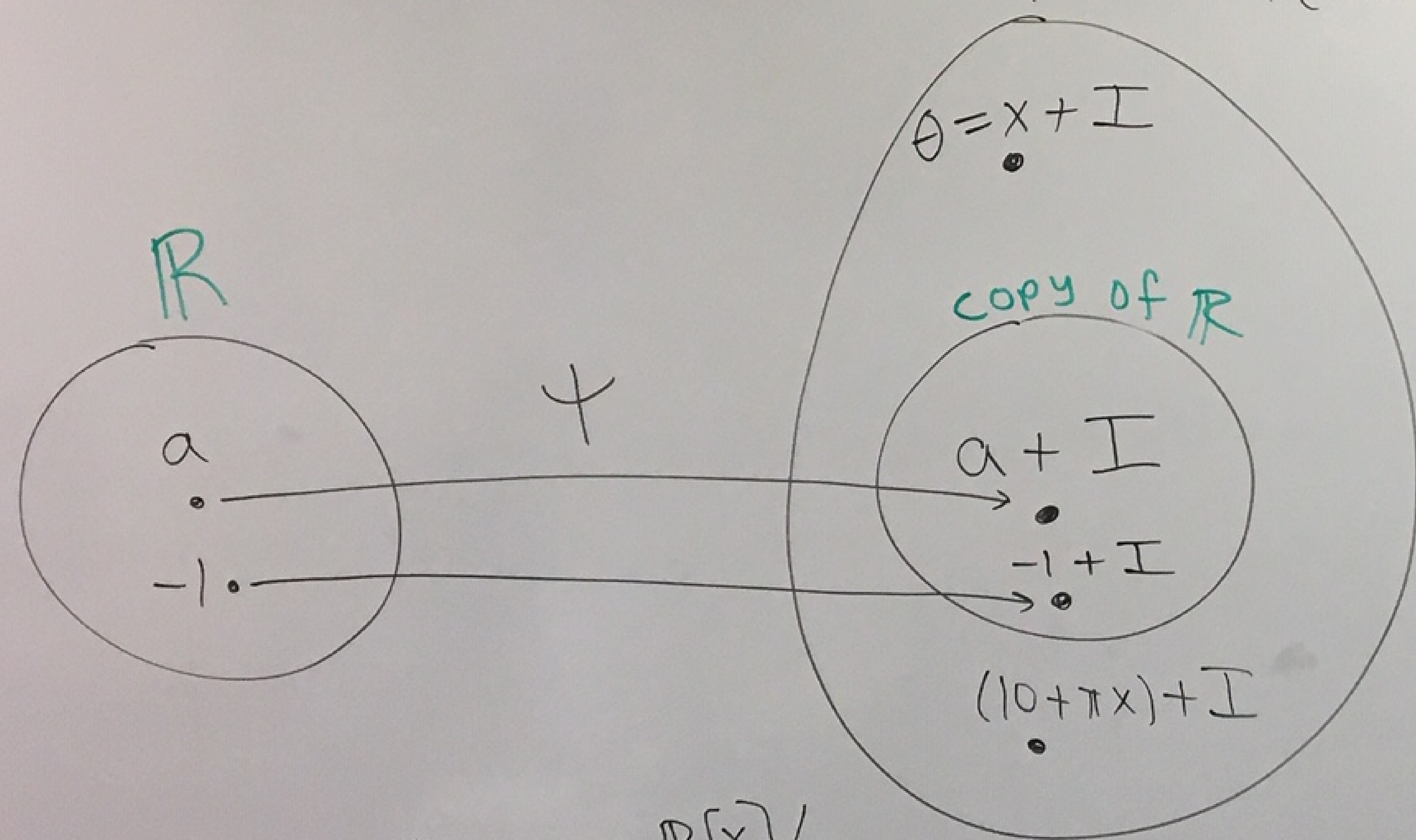
pf: Let $f(x)+I \in K$ where $f(x) \in \mathbb{R}[x]$.
By the division alg., $f(x) = (x^2+1)q(x) + r(x)$
where $q(x), r(x) \in \mathbb{R}[x]$ and $r(x) = ax+b$
where $a,b \in \mathbb{R}$.

So,
$$f(x) - r(x) = (x^2+1)q(x) \in I.$$

So,
$$\begin{aligned} f(x)+I &= r(x)+I \\ &= (a+bx)+I. \end{aligned}$$

$\boxed{\text{Claim}}$

$K = \mathbb{R}[x]/(x^2+1) = \mathbb{R}[x]/I$



$\psi : \mathbb{R} \to \mathbb{R}[x]/I$

$\psi(a) = a + I$

ψ is 1-1 and onto the subfield $\{a + I \mid a \in \mathbb{R}\}$ in K.

K is isomorphic to $\mathbb{C}$

$(a+bx)+I \longleftrightarrow a+bi$

Let $\theta = x + I$

Then,

$$\theta^2 = (x+I)(x+I) = x^2 + I = -1 + I$$

$\boxed{x^2 - (-1) = x^2 + 1 \in I}$

So, "$\theta^2 = -1$"

So, θ acts like i.