① 2008-09-09 Alg notes

Ring = comm ring w/unity unless stated otherwise

$\boxed{\text{Ideal}}$: subset $I \subset R$ we can mod out by to get R/I

additively $+$: subgroup of abelian group, closed subset under

multiplicatively: $*$

→ kernel of ring homomorphism (iso thm)

→ set that "acts like" 0

should get same answer

<u>kernel</u> $a \in I \Rightarrow ab \in I$ for any $b \in R$

$$f(ab) = f(a)f(b) = 0f(b) = 0 \quad ✓$$

so f homomorphism $\Rightarrow$ kernel "absorbs" under $*$

<u>set like 0</u> $a \in I \Rightarrow ab \in I$ for any $b \in R$

a "=" 0 then ab "=" 0 any b ✓

$\boxed{\text{prime, maximal ideals}}$

recall set version of prime:

I = all multiples of p $\subset \mathbb{Z}$

p prime: $ab \in I \Rightarrow a \in I$ or $b \in I$

define ideal I <u>prime</u> if above property.

Zero ideal $(0) \subset R$ prime $\Leftrightarrow$

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

so R is an integral domain

$I \subset R$ maximal ideal if R/I has no ideals other than $(0), (1)$

$\Leftrightarrow$ no ideal $I \subset J \subset R$ strictly between.

(If $I \subset J \subset R$ then $(0) \subset \bar{J} \subset R/I$)

image of I image of J

---

maximal $\Rightarrow$ prime

I maximal $\Leftrightarrow$ R/I is a field (division)

---

idea: let $a \in R$.

Either
- $(a) \subset R$ is an ideal not containing 1
- $(a) \subset R$ is an ideal containing 1

$ab = 1 \Leftrightarrow b = a^{-1}$

So (0) is only ideal not containing 1 $\Leftrightarrow$ every $a \neq 0$ in R has an inverse.

proves both, if one believes iso thms

Naturalist view of $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

we can't "make up" numbers, we reveal properties of what's there.

constructive, abstract view:

If we can build it, it's there. (finite fields)

solutions to poly equs $ax^2+bx+c=0$ $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$
like ODE's generalize $\frac{df}{dx}=g$, one thought general
solutions to poly equs generalize radicals. not so ($\deg \geq 5$)

Looking in $\mathbb{C}$, algebraic -vs- transcendental

$\mathbb{C}$ is immensely infinite vector space / $\mathbb{Q}$ (counting)

Given $a \in \mathbb{C}$, look at all linear combinations of powers of a.

$\mathbb{Q}[a] \subset \mathbb{C}$ spanning set $1, a, a^2, a^3, a^4, \ldots$

$\mathbb{Q}[a]$ = all polys in a w/ coefs in $\mathbb{Q}$

(compare $\mathbb{Q}[x]$ = " " x " " where x is a variable)
what you get starting w/ $\mathbb{Q}, x$, using $+, *$

---

case
- $\mathbb{Q}[a]$ infinite dim / $\mathbb{Q}$ (transcendental)
- $\mathbb{Q}[a]$ finite dim / $\mathbb{Q}$ (algebraic)

$\exists$ linear dependence $a^d \in$ subspace gen by $1, a, \ldots, a^{d-1}$

$$\iff a^d = c_0 + c_1 a + c_2 a^2 + \ldots + c_{d-1} a^{d-1}$$

(for $c_i \in \mathbb{Q}$)

$$\iff a^d - c_{d-1} a^{d-1} - \ldots - c_1 d - c_0 = 0$$

in which case any higher power also

$a^{d+e} = a^d a^e = (c_0 + \ldots + c_{d-1} a^{d-1}) a^e$ lowers degree

so either
$\nearrow$ $1, a, a^2, \ldots$ linearly indep / $\mathbb{Q}$
$\searrow$ $1, a, a^2, \ldots a^{d-1}$ indep, $a^d \in$ previous,
$\mathbb{Q}[a]$ is d-dim space / $\mathbb{Q}$

(compare $\mathbb{C} = \mathbb{R}[i]$ is 2-dim / $\mathbb{R}$)

---

we can construct such fields from scratch:

Given a algebraic over $\mathbb{Q}$,

let $f(x) = x^d - c_{d-1}x^{d-1} - \ldots - c_1 x - c_0$

be unique poly of min degree so $f(a) = 0$.

Then
- f is prime
- (f) is prime ideal
- $\mathbb{Q}[x]/(f) \cong \mathbb{Q}[a]$

$$\mathbb{Q}[x] \longrightarrow \mathbb{C}$$
$$\mathbb{Q} \mapsto \mathbb{Q}$$
$$x \mapsto a$$

has kernel f, image $\mathbb{Q}[a]$

---

matrices, finite fields