Notes

December 1, 2014

5.2 #13

if $\varphi : \mathbb{Z} + \mathbb{Z} \to \mathbb{Z}$ is a ring homomorphism then for every $m, n \in \mathbb{Z}$ we have $\varphi(m,n) = \varphi((m,0) + (0,n)) = \varphi(m,0) + \varphi(0,n) = \varphi(\underbrace{1+1+\cdots+1}_{m}, 0) + \varphi(0, \underbrace{1+1+\cdots+1}_{n}) = \underbrace{\varphi(1,0)+\ldots\varphi(1,0)}_{m} + \underbrace{\varphi(0,1)+\ldots\varphi(0,1)}_{n} = m\varphi(1,0) + n\varphi(0,1)$

now $\alpha = \varphi(1,0)$ and $\beta = \varphi(0,1)$ and $\alpha + \beta = \varphi(1,1) = 1$ and so $\alpha + \beta = 1$
also $\alpha\beta = \varphi(0,0) = 0$.

1. $\alpha = 0$ then $\beta = 1$ and so $\varphi(m,n) = m \cdot 0 + n \cdot 1 = n$ which is a ring homomorphism
2. $\beta = 0$ then $\alpha = 1$ and so $\varphi(m,n) = m$ which is a ring homomorphism.

we start with a homomorphism, check all possible outputs and check that all outputs are homomorphisms.

last time

$\varphi : R \to S$ is a ring hom
$\ker\varphi = x \in R : \varphi(x) = 0$
$R/\ker\varphi = \{[x] : x \in R\}$
$x \sim y \Leftrightarrow x - y \in \ker\varphi$
$\Leftrightarrow \varphi(x) = \varphi(y)$

5.3

definition

given a comm ring R and a non-empty subset $I \subseteq R$ we say that I is an **ideal** of(in) R if

1. for every two elements $x, y \in I$ we have $x + y, x - y \in I$ in particular $0 \in I$.
2. for every $r \in R$ and every $x \in I$ we have $rx \in I$

examples

every commutative ring has at least two ideals (unless $0 = 1$)
$\{0\}$ is an ideal of R
R is an ideal of R.
if these are the only possible ideals then R is a field

thrm

let R be a commutative ring. then R is a field if and only if $\{0\}$ and R are the only ideals of R.

proof

$\Rightarrow$ assume that R is a field, and let I be an ideal of R. if $I = \{0\}$ we are done so assome $I \neq \{0\}$. we want to prove that $I = R$. let $x \neq 0 \in I$. because R is a field then $x^{-1} \in R$ and $x^{-1}x \in I$ because $x \in I$ and so $1 \in I$ and $r = r \cdot 1 \in I$ and so $I = R$

$\Leftarrow$ Take $a \neq 0 \in R$. we want to prove that a is invertible. $I = \{ra : r \in R\} \subseteq R$

claim: I is an ideal of R. Now we have an ideal different from zero because $a \in I$ therefor $I = R$ and so $1 \in I$. $\exists r \in R$ such that $ra = 1$ and so $r = a^{-1}$.

observation

1. given $a \in R$ then $\{ra : r \in R\}$ is an ideal of R denoted Ra or (a) or aR. In fact this is the smallest ideal of R that contains a.

   we call this the ideal generated by a.

2. $1 \in I$ iff $I = R$.

definition

for R commutative ring, we say the R is a **principle ideal** if every ideal of R is principal. that is every ideal of R is of the form (a)

definition

we say that R is a **principal ideal domain** (PID) if R is an integral domain and a principal ideal ring.

example

fields are always principal ideal rings generated by 1 (and PID).

$\mathbb{Z}$ is a PID.

example 5.3.1

let $I \in \mathbb{Z}$ be an ideal different from 0. Let $a \in I$ be the smallest positive integer in I. (note that there is an element not zero in I and so if there is a negative in I then it's additive inverse is in I.

$\supseteq$

$a \in I \rightarrow ra \in I$

$\subseteq$

pick some $x \in I$ $x = qa + r$ where $0 \leq r < 0$ then $r = x + -q(a)$ and because $a \in I$ then $-qa \in I$ and $r \in I$ and so $r = 0$ and so $x \in (a)$

examples

let K be a field then $K[x]$ is a PID.

let $I \subseteq K[x]$ be a nonzero ideal. let $q(x) \in I$ be a non-zero polynomial of minimal degree

claim:$I = (q(x))$

proof

$q(x)K[x] \subseteq I$ is clear

let $f(x) \in I$. $f(x) = b(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg q(x)$

but $r(x) = f(x) + (-b(x)q(x)) \in I$ of course $q(x)$ has minimal degree and so by this choice we must have $r(x) = 0$ and so $f(x)$ is a multiple of $q(x)$ and we are done.