2/21 HW

HW #1, #8

Let R be a ring with identity $1 \neq 0$
Let $R^\times$ be the units of R
Prove that $R^\times$ is a group under mult.

Proof: "If $a, b \in R^\times$, then $ab \in R^\times$" ← need to prove
closure Let $a, b \in R^\times$ so a^{-1}, b^{-1} exist
I claim that $ab \in R^\times$, that is ab is a unit

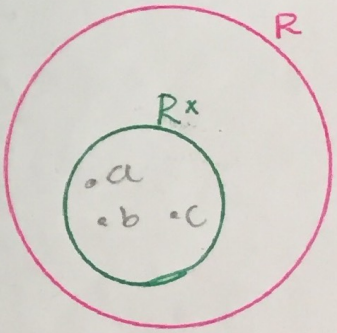
Note that: $(ab)(b^{-1}a^{-1}) = 1$
$(b^{-1}a^{-1})(ab) = 1$

so $b^{-1}a^{-1}$ is the inverse of ab. So ab is a unit, Thus $ab \in R^\times$

$R = \mathbb{Z}_8$

$\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

Associativity
Let $a, b, c \in R^\times$
Then $a, b, c \in R$ and since R is associative
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$



(alternative)
since $R^\times \subseteq R$ and R has the associative property since R is a ring so does $R^\times$

identity
1 is a unit so $1 \in R^\times$

inverse
Let $a \in R^\times$ Then $a^{-1} \in R$ exists
and a^{-1} is a unit too!!! so, $a^{-1} \in R^\times$
↑ (since $aa^{-1} = 1 = a^{-1}a$)

□

Test #1 is on
HW #1–3

HW # 3 #6(c)

Let R be an integral domain
Then the unit of $R[x]$ are $R^\times$

example

units of $\mathbb{Z}_7[x]$

$\mathbb{Z}_7[x] = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, x, x+3, \bar{5}x^2+\bar{2}, \bar{2}x+\bar{6}, \dots\}$

$\mathbb{Z}_7^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$(\mathbb{Z}_7[x])^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$\mathbb{Z}_8$ is not an integral domain since $\bar{2}\cdot\bar{4} = \bar{0}$

Proof: Let $f, g \in R[x]$ with $f \neq 0, g \neq 0$

Suppose $fg = 1$ in $R[x]$, ie f and g are units in $R[x]$

By part (a),

$$\underbrace{\deg(f)}_{\geq 0} + \underbrace{\deg(g)}_{\geq 0} = \deg(fg) = \deg(1) = 0$$

So $\deg(f) = \deg(g) = 0$

That is $f, g \in R$

since $fg = 1$, $f, g \in R^\times$ ☒

* Doesn't work in $\mathbb{Z}_8[x]$

$(\bar{1} + \bar{4}x)(\bar{1} + \bar{4}x) =$

$\bar{1} + \underbrace{\bar{8}x}_{\bar{8}=\bar{0}} + \underbrace{\bar{16}x^2}_{\bar{16}=\bar{0}} = \bar{1}$

$\bar{1} + \bar{4}x$ is a unit in $\mathbb{Z}_8[x]$

$\mathbb{Z}_8$ is not an integral domain

P.1 2/21 Tuesday Week 5 Feb. 21. 2017

Ideals of Rings

- Ideal generalizes normal subgroups.

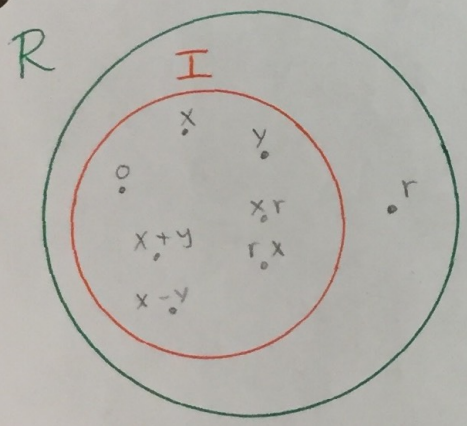
Def: Let R be a ring, Let $I \subseteq R$. We say that I is an **ideal** of R if

(1) I is a subgroup of R under $+$

(2) For every $r \in R$ and $x \in I$ we have that $rx \in I$ and $xr \in I$

(comment on (1))
R is an abelian group under $+$ (ring axiom)
So I is a normal subgroup under $+$

(another way for (2))
For every $r \in R$
$rI \subseteq I$ and $Ir \subseteq I$
where $rI = \{rx \mid x \in I\}$ $\quad Ir = \{xr \mid x \in I\}$

- 

From 4550
a subgroup of an abelian group is a normal subgroup

Example:
Let $n \geq 1$. Let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$
Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proof:

- (1) $0 = n \cdot 0 \in n\mathbb{Z}$
given $x = nk$ and $y = nl$ where $k, l \in \mathbb{Z}$
then $x - y = n(k - l) \in n\mathbb{Z}$

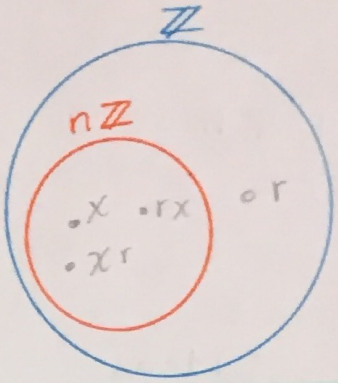
] $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

(2) Let $x \in n\mathbb{Z}$ and $r \in \mathbb{Z}$

so $x = nk$ where $k \in \mathbb{Z}$

Then $rx = n(rk) \in n\mathbb{Z}$

and $xr = n(rk) \in n\mathbb{Z}$



From 4550

a subgroup

$N \trianglelefteq G$, +

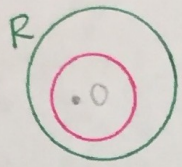
(1) $N \leq G$

(2) $g+N = N+g$

$\forall g \in G$

Note:

Let R be a ring



R has at least these ideals:

(1) $\{0\}$ ← the trivial ideal or the zero ideal

(2) R ← The entire ring

Tuesday's 3:03pm Theorem about the ideals of $\mathbb{Z}$

Let I be an ideal of $\mathbb{Z}$, Then $I = n\mathbb{Z}$ where $n \geq 0$

All the ideals of $\mathbb{Z}$:

$0\mathbb{Z} = \{0\}$

$1\mathbb{Z} = \mathbb{Z}$

$2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

⋮ ⋮

Proof:

Let I be an ideal of $\mathbb{Z}$

By Math 4550, since I is a subgroup of $\mathbb{Z}$ and $\mathbb{Z}$ is cyclic, I must be cyclic, so $I = n\mathbb{Z}$ where $n \geq 0$.

when $n = 0$, $I = \{0\}$ is an ideal of $\mathbb{Z}$

when $n \geq 1$, we just proved that $I = n\mathbb{Z}$ is an ideal.

So thats all the ideals of $\mathbb{Z}$ ☆

Thursday Week 5 Feb. 23. 2017

Def: Let R be commutative ring with identity $1 \neq 0$

(1) Let $a \in R$. The **ideal generated by a** is

$$\langle a \rangle = Ra = aR = \{ra \mid r \in R\}$$

↳ in HW you prove this is an ideal

(2) Given an ideal I of R we say that I is a **principal ideal** if $\exists\ a \in R$ with $I = \langle a \rangle$

(3) If R is an integral domain and every ideal of R is principal then we call R a **principal ideal domain** or **PID**

Ex: $2\mathbb{Z} = \{2r \mid r \in \mathbb{Z}\}$ is a principal ideal of $\mathbb{Z}$ you can write it as $\langle 2 \rangle$

Ex: $\mathbb{Z}$ is a PID because

(1) $\mathbb{Z}$ is an integral domain

(2) every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = \langle n \rangle$ where $n \geq 0$, That is, every ideal of $\mathbb{Z}$ is a principal ideal (we proved this last time)

Ex: In hw you will show that every ideal of $\mathbb{Z}_n$ is principal. So, $\mathbb{Z}_p$ is a PID if p is prime (need prime to get an integral domain.)

Ex: In $R = \mathbb{Z}_3[x]$ we have

$$\langle x + \bar{1} \rangle = \{(x+\bar{1}) f(x) \mid f(x) \in \mathbb{Z}_3[x]\}$$

$$= \{(x+\bar{1})\cdot\bar{0},\ (x+\bar{1})\cdot\bar{1},\ (x+\bar{1})\cdot\bar{2},\ (x+\bar{1})(x),\ (x+\bar{1})(x+\bar{1}),$$
$$(x+\bar{1})(x+\bar{2}),\ (x+\bar{1})(\bar{2}x),\ldots,\ (x+\bar{1})(x^{100}+\bar{2}x+\bar{1})\ldots\}$$

$F[x]$

$\langle x+1 \rangle \neq \langle x \rangle + \langle 1 \rangle$

Division Algorithm for F[x]

Let F be a field

Let $f(x)$ and $g(x)$ be in $F[x]$, with $g(x)$ not the zero polynomial.

Then there exists unique $q(x)$ and $r(x)$ from $F(x)$ where $g(x)q(x)+r(x)$

and either $r(x)=0$ or $\deg(r(x)) < \deg(g(x))$

Ex: Divide $g(x)$: $\bar{2}x+\bar{1}$ into $f(x)$: $x^3+x+\bar{1}$ in $\mathbb{Z}_3[x]$

$\mathbb{Z}_3$ is a field

$$\begin{array}{r|l} \bar{2}x+\bar{1} & \bar{2}x^2+\bar{2}x+\bar{1} \quad q(x) \\ & x^3+x+\bar{1} \\ & -(x^3+\bar{2}x^2) \\ \hline & x^2+x+\bar{1} \\ & -(x^2+\bar{2}x) \\ \hline & \bar{2}x+\bar{1} \\ & -(\bar{2}x+\bar{1}) \\ \hline & \bar{0} \quad r(x) \end{array}$$

$\rightarrow \bar{2}\cdot\bar{2}=\bar{4}=\bar{1}$

$\rightarrow -\bar{2}x^2 = x^2$

$-\bar{2}=1$

$$x^3+x+\bar{1} = (\bar{2}x+\bar{1})(\bar{2}x^2+\bar{2}x+\bar{1})+\bar{0}$$

$$f(x) = g(x)\cdot q(x) + r(x)$$

Big Theorem Thursday

Let F be a field, Then $F[x]$ is a PID

Proof: We already know that $F[x]$ is an integral domain because F is an integral domain. Let I be an ideal of $F[x]$

We need to show that I is principal.

If $I = \{0\}$, then $I = \langle 0 \rangle$. So I is principal.

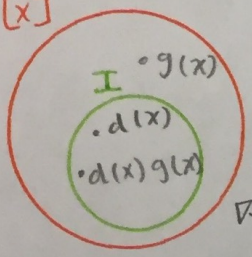
Suppose $I \neq \{0\}$

So I contains at least one non-zero element.

Let $d(x)$ be a non-zero polynomial with minimal degree from I.

That is, $d(x) \in I$ and

$$\deg(d(x)) \leq \deg(f(x)) \quad \forall f(x) \in I - \{0\} \qquad (*)$$



claim: $I = \langle d(x) \rangle$

proof of claim: ($\langle d(x) \rangle \subseteq I$)

Note that $\langle d(x) \rangle = \{d(x)\, g(x) \mid g(x) \in F[x]\}$

If $g(x) \in F[x]$ and $d(x) \in I$ then $d(x)g(x) \in I$ because I is an ideal

so, $\langle d(x) \rangle \subseteq I$

($I \subseteq \langle d(x) \rangle$), Let $f(x) \in I$

By the division algorithm there exists $q(x), r(x) \in F[x]$ where $f(x) = d(x)q(x) + r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(d(x))$

Note that $r(x) = \underbrace{f(x)}_{\text{in } I} - \underbrace{\underbrace{d(x)}_{\text{in } I}\ \underbrace{q(x)}_{\text{in } F[x]}}_{\text{in } I} \in I$

By (*) and the fact that $r(x) \in I$ we cannot have that $\deg(r(x)) < \deg(d(x))$. So $r(x) = 0$

Thus $f(x) = d(x)q(x) \in \langle d(x) \rangle$

so $I \subseteq \langle d(x) \rangle$. ∎