HW 2/7

HW #1 Review

#1 (d) part c

in # theory this is called a # field.

First show $\mathbb{Q}(\sqrt{2})$ is a ring with $1 = 1 + 0\sqrt{2}$

→ Find the units of the ring

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \{1 = 1 + 0\sqrt{2}, \frac{1}{2} - \frac{3}{10}\sqrt{2}, \ldots\}$

Let $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ with $a + b\sqrt{2} \neq 0$.

let's show $\frac{1}{a+b\sqrt{2}} \in \mathbb{Q}(\sqrt{2})$

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

mult. by the conjugate

This is in $\mathbb{Q}(\sqrt{2})$ as long as $a^2 - 2b^2 \neq 0$.

Suppose $a^2 - 2b^2 = 0$ we show this leads to a contradiction.

Case 1 $\quad b = 0$

If so, then $a^2 - 2b^2 = 0$ becomes $a^2 = 0$
then $a = 0$. Then $a + b\sqrt{2} = 0$
contradiction

Case 2 $\quad b \neq 0$

Then $a^2 - 2b^2 = 0$ becomes $\left(\frac{a}{b}\right)^2 = 2$

Then $\frac{a}{b} = \pm\sqrt{2}$ which can't happen because $\sqrt{2} \notin \mathbb{Q}$

▨

Def: Let $n>1$

- $\mathbb{Z}_n^\times = \{\bar{x} \in \mathbb{Z}_n \mid \bar{x}$ is not a zero divisor and $\bar{x} \neq \bar{0}\}$

  $\underset{\uparrow}{=} \{\bar{x} \in \mathbb{Z}_n \mid \gcd(x,n)=1\}$

  from last time

Ex: $\mathbb{Z}_6^\times = \{\bar{1}, \bar{5}\}$, $\mathbb{Z}_{10}^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

Number Theory Theorem:
Let $a, b \in \mathbb{Z}$, not both 0, and let $d = \gcd(a,b)$.
Then $\exists\, x, y \in \mathbb{Z}$ with $ax + by = d$

Ex: $a=3$, $b=2$

$d = \gcd(3,2) = 1$

$3(1) + 2(-1) = 1$

$\uparrow a\ \uparrow x\ + \uparrow b\ \uparrow y = \uparrow d = \gcd(2,3)$

- **Theorem:** $\mathbb{Z}_n^\times$ is the set of units of $\mathbb{Z}_n$.

* $\bar{x}$ is a <u>unit</u> in $\mathbb{Z}_n$ if $\exists\, \bar{y} \in \mathbb{Z}_n$ with $\bar{x}\bar{y} = 1$
we call $\bar{y} = \bar{x}^{-1}$

* $\bar{n} = \bar{0}$
$n \equiv 0 \pmod n$
$n \mid (n-0)$ ✓

Proof: Let U be the set of units in $\mathbb{Z}_n$
Let's prove that $U = \mathbb{Z}_n^\times$

($\Leftarrow$) Let $\bar{a} \in \mathbb{Z}_n^\times$
Then $\bar{a} \neq \bar{0}$ and $\gcd(a,n) = 1$
By the # theory theorem $\exists\, x, y \in \mathbb{Z}$ with $ax + ny = 1$. Then $\bar{a}\bar{x} + \bar{n}\bar{y} = \bar{1}$ in $\mathbb{Z}_n$
Since $\bar{n} = \bar{0}$, we have $\bar{a}\bar{x} = \bar{1}$, so $\bar{a}$ is a unit
Thus $\bar{a} \in U$, so $\mathbb{Z}_n^\times \subseteq U$

($\Rightarrow$) Let $\bar{b} \in U$, Then $\bar{b} \neq \bar{0}$ and $\exists\, \bar{b}^{-1} \in \mathbb{Z}_n$ with $\bar{b}\bar{b}^{-1} = \bar{b}^{-1}\bar{b} = 1$
Let's show $\bar{b}$ is not a zero divisor

- Suppose $\bar{b}\bar{x} = \bar{0}$ where $\bar{x} \in \mathbb{Z}_n$
  Then $\bar{b}^{-1}\bar{b}\bar{x} = \bar{b}^{-1}\bar{0}$, so $\bar{x} = \bar{0}$
  Thus $\bar{b}$ is NOT a zero divisor

$\bar{b}$ is a zero divisor means $\bar{b} \neq \bar{0}$ and $\exists\, \bar{x} \in \mathbb{Z}_n$ with $\bar{x} \neq \bar{0}$ and $\bar{b}\bar{x} = \bar{0}$

Therefore, $\bar{b} \in \mathbb{Z}_n^\times$ so $U \subseteq \mathbb{Z}_n^\times$, $\therefore$ we are done & $U = \mathbb{Z}_n^\times$

Corollary:

$\mathbb{Z}_p$ is a field if p is prime

Proof: Suppose p is prime

Then from last time $\mathbb{Z}_p$ is an integer domain

Also the units are $\mathbb{Z}_p^{\times} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$\uparrow$

$\{\bar{x} \mid \bar{x} \neq \bar{0}, \gcd(x,p)=1\}$

int. domain

- commutative ring w/ $1 \neq 0$
- no zero divisor

from the theorem we just proved

So, $\mathbb{Z}_p$ is a field since every non-zero element is a unit. $\boxtimes$

Theorem: Let F be a field. Then F is an integer domain.

Proof: Let F be a field. Then F is commutative with identity $1 \neq 0$. To show that F is an integral domain all that's left is to show that F has no zero divisors.
Let $x \in F$ with $x \neq 0$. we show x is not a zero divisor.

Suppose $y \in F$ where $xy = 0$

Since $x \neq 0$ and F is a field, x^{-1} exists in F.

So $x^{-1} x y = x^{-1} 0$.

Thus, $y = 0$. so x can't be a zero divisor. ☒

Is this true?

"If R is an integral domain, then R is a field"

NO! $R = \mathbb{Z}$ is an integral domain but not a field.

^ counterexample

Theorem: If R is a finite integral domain, then R is a field.

lemma:

Let S be a <u>finite</u> set and $f: S \to S$

then f is 1-1 iff f is onto

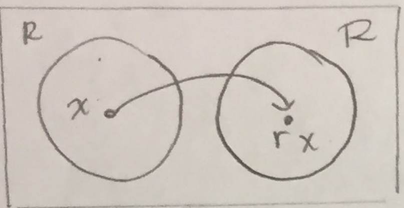
Proof of Theorem:

Let R be a finite integral domain, then R is commutative and has an identity $1 \neq 0$.
We have to show that every non zero element of R is a unit in order to prove that R is a field.

Suppose $R = \{0, 1, \underbrace{r_1, r_2, \ldots, r_n}_{r \text{ is one of these guys}}\}$.

Let r be one of the r_i.

Let $f_r : R \to R$ where $f_r(x) = rx$.



Let's show that f_r is 1-1.

Suppose $f_r(x) = f_r(y)$ for some $x, y \in R$

Then $rx = ry$

so $rx - ry = 0$

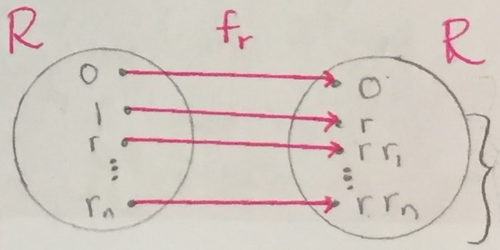
then $r(x-y) = 0$

$r \neq 0$

since $r \neq 0$ and R is an integral domain

we must have $x - y = 0$

$\therefore x = y$



since f is onto and $1 \in R$, then one of these guys is 1.

Thus, f is 1-1

So by our lemma f is onto.

So $\exists\ r_k$ where $f_r(r_k) = 1$

That is, $rr_k = 1$. So, r is a unit

So every non-zero element of R is a unit $\therefore$ R is a field $\boxtimes$

This argument does not work for infinite sets.

P.2 2/9

Polynomial Rings

Let R be a commutative ring with identity $1 \neq 0$.
Then $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \geq 0\}$ is called the **ring of polynomials** in the variable x with coefficients from R.

Facts:

- $R[x]$ is a ring
- Addition and multiplication in $R[x]$ are done in the usual way.
- The additive identity of $R[x]$ is the additive identity 0 of R
- The multiplicative identity of $R[x]$ is the multiplicative identity 1 of R
- If R is a commutative ring with $1 \neq 0$, then $R[x]$ is commutative with $1 \neq 0$.

Def:
Given $f(x) = a_n x^n + a_{n+1}x^{n+1} + \cdots + a_1 x + a_0 \in R[x]$ with $a_n \neq 0$, then the **degree** of f is n. We write $\deg(f) = n$.
The only special case is that $\deg(0)$ is undefined.

units of $\mathbb{Z}_3$

Ex: $R = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

degree is 0 degree is 1

$\mathbb{Z}_3[x] = \{\bar{0}, \boxed{\bar{1}, \bar{2}}, x, \bar{1} + x, \bar{2} + x, \bar{2}x, \bar{1} + \bar{2}x,$

degree is undefined units of $\mathbb{Z}_3[x]$

$\bar{1} + \bar{2}x + x^2, \ldots, \bar{2}x^{100,000,000} + \bar{2}x^3 + x, \ldots\}$

degree is 2 degree is 100,000,000 infinitely many more polynomials.

Ex: $(\bar{1}+\bar{2}x+x^2)+(\bar{2}+\bar{2}x+\bar{2}x^2) = \underset{\bar{0}}{\bar{3}} + \underset{x}{\bar{4}x} + \underset{\bar{0}}{\bar{3}x^2} = x$

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

Theorem:

Let R be an **integral domain**. Let $P(x)$ and $q(x)$ be non zero elements of $R[x]$. Then:

(1) $\deg(P(x)q(x)) = \deg(P(x)) + \deg(q(x))$

(2) The units of $R[x]$ are the units of R

(3) $R[x]$ is an integral domain

Ex: $\mathbb{Z}_4$ is not an integral domain in $\mathbb{Z}_4[x]$

$$\underset{\text{deg } 1}{(\bar{2}x)}\,\underset{\text{deg } 1}{(\bar{2}x)} = \bar{4}x = \underset{\text{undefined degree}}{\bar{0}}$$

$\mathbb{Z}_4[x]$ is not an integral domain