SOLUTIONS TO LECTURE 25 PROBLEMS 97–102

P97 #11 p. 261

In $\mathbb{Z}$ find $a \in \mathbb{N}$ such that
$$\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$$
$$\langle a \rangle = \langle 3 \rangle + \langle 6 \rangle$$
$$\langle a \rangle = \langle m \rangle + \langle n \rangle$$

(a.) $\langle 2 \rangle + \langle 3 \rangle = \{ 2s + 3t \mid s, t \in \mathbb{Z} \}$

Observe $3 - 2 = 1$ and $x = x(1) = 3x - 2x$

that is, $x = 2(-x) + 3(x) \Rightarrow \langle 2 \rangle + \langle 3 \rangle = \mathbb{Z}$

So, $\boxed{\langle 1 \rangle = \langle 2 \rangle + \langle 3 \rangle}$

(b.) $\langle 3 \rangle + \langle 6 \rangle = \{ 3s + 6t \mid s, t \in \mathbb{Z} \}$
$= \{ 3(s + 2t) \mid s, t \in \mathbb{Z} \}$
$= \boxed{\langle 3 \rangle}$ (note, $\langle 6 \rangle \subseteq \langle 3 \rangle$ since $x \in \langle 6 \rangle \Rightarrow x = 6k = 3(2k) \in \langle 3 \rangle$)

(C.) By Bezout's Th^{m} if $d = \gcd(m,n)$ then $\exists k, l \in \mathbb{Z}$ such that $km + ln = d \Rightarrow d \in \langle m \rangle + \langle n \rangle$

If $0 < a' < d$ had $\langle a' \rangle = \langle m \rangle + \langle n \rangle$ then we would find $a' \in \langle a' \rangle = \langle m \rangle + \langle n \rangle \supseteq \langle d \rangle$ ← included in $\langle m \rangle + \langle n \rangle$

thus $d \in \langle a' \rangle \Rightarrow d = a'k$ for some $k \in \mathbb{N}$

But, $a' < d$ so this is impossible. Hence

$$\boxed{\langle d \rangle = \langle \gcd(m,n) \rangle = \langle m \rangle + \langle n \rangle}$$

Oh, so my argument thus far only shows that $\langle d \rangle \subseteq \langle m \rangle + \langle n \rangle$ as $\tilde{k}d = \tilde{k}(km + ln) = \underbrace{\tilde{k}km + \tilde{k}ln}_{\text{in } \langle m \rangle + \langle n \rangle}$.

Converely, if $mx + ny \in \langle m \rangle + \langle n \rangle$ we ought to show $mx + ny \in \langle d \rangle$. But, $d \mid m$ and $d \mid n$ as it is a common divisor, so $\exists \alpha, \beta \in \mathbb{Z}$ s.t. $m = d\alpha$ and $n = d\beta$

consequently, $mx + ny = d\alpha x + d\beta y = d(\alpha x + \beta y) \in \langle d \rangle$

Thus we've shown $\langle d \rangle = \langle m \rangle + \langle n \rangle$ where $d = \gcd(m,n)$.

P98 # 28 from p. 261 of Gallian

Let $R = \mathbb{Z}_8 \times \mathbb{Z}_{30}$ find each maximal ideal I of R, identity the size of each field R/I

Notice $|R| = 8(30) = 240$

$|I| = 120$ given if $I = \langle (a,b) \rangle$ where $\operatorname{lcm}(|a|,|b|) = 120$

Let $a = 1$, $b = 2$ to achieve $|a| = 8$, $|b| = 15$

So $I = \langle (1,2) \rangle$ provides $R/I \approx \mathbb{Z}_2$

aka $\dfrac{\mathbb{Z}_8 \times \mathbb{Z}_{30}}{\mathbb{Z}_8 \times 2\mathbb{Z}_{30}} \approx \dfrac{\mathbb{Z}_{30}}{2\mathbb{Z}_{30}} \approx \mathbb{Z}_2$. Again $\boxed{I = \mathbb{Z}_8 \times 2\mathbb{Z}_{30}}$ maximal

Likewise, $\dfrac{\mathbb{Z}_8 \times \mathbb{Z}_{30}}{2\mathbb{Z}_8 \times \mathbb{Z}_{30}} \approx \dfrac{\mathbb{Z}_8}{2\mathbb{Z}_8} \approx \mathbb{Z}_2$

$\boxed{J = 2\mathbb{Z}_8 \times \mathbb{Z}_{30} = \langle (2,1) \rangle.}$ maximal

To obtain $|R/K| = 3$ need $|K| = 80$

$\underbrace{\boxed{K = \mathbb{Z}_8 \times 3\mathbb{Z}_{30}}}_{\text{maximal}}$ gives $\dfrac{\mathbb{Z}_8 \times \mathbb{Z}_{30}}{\mathbb{Z}_8 \times 3\mathbb{Z}_{30}} \approx \dfrac{\mathbb{Z}_{30}}{3\mathbb{Z}_{30}} \approx \mathbb{Z}_3$.

field $\Rightarrow \mathbb{Z}_8 \times 3\mathbb{Z}_{30}$ was maximal.

Additionally, $L = \mathbb{Z}_8 \times 5\mathbb{Z}_{30}$ provides

$\dfrac{\mathbb{Z}_8 \times \mathbb{Z}_{30}}{\mathbb{Z}_8 \times 5\mathbb{Z}_{30}} \approx \dfrac{\mathbb{Z}_{30}}{5\mathbb{Z}_{30}} \approx \mathbb{Z}_5$ $\therefore$ $\boxed{\mathbb{Z}_8 \times 5\mathbb{Z}_{30} \text{ maximal}}$

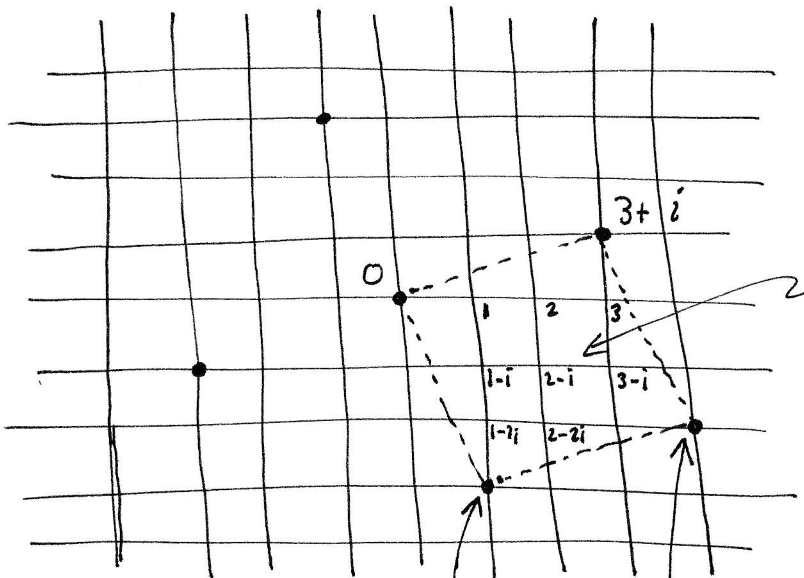
field.

P 99 # 29 of p. 261

How many elements are in $\mathbb{Z}[i]/\langle 3+i\rangle$?

As we've shown (a bit later) any generator of the ideal $\langle 3+i\rangle$ is an associate of $3+i$.
As $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ this means

$3+i, \ -3-i, \ 3i-1, \ -3i+1$ are the smallest elements in $\langle 3+i\rangle$



this cell contains a rep. of each coset.

$-3i+1$ $\qquad$ $-2i+4 = (-3i+1)+(3+i)$

Hence, by the picture, setting $I = \langle 3+i\rangle$,

$$\boxed{\mathbb{Z}[i]/\langle 3+i\rangle = \{I, 1+I, 2+I, 3+I, 1-i+I, 2-i+I, 3-i+I, 1-2i+I, 2-2i+I, 3-2i+I\}}$$

I find <u>10 elements.</u>

<u>Remark:</u> you are free to argue as Gallian does in the answers in back of book. I just prefer this geometric approach.

P100 # 34 of p. 262

Prove that $\langle 2+2i \rangle$ is <u>not</u> a prime ideal of $\mathbb{Z}[i]$.
How many elements are in $\mathbb{Z}[i]/\langle 2+2i \rangle$?
What is the characteristic of $\mathbb{Z}[i]/\langle 2+2i \rangle$?

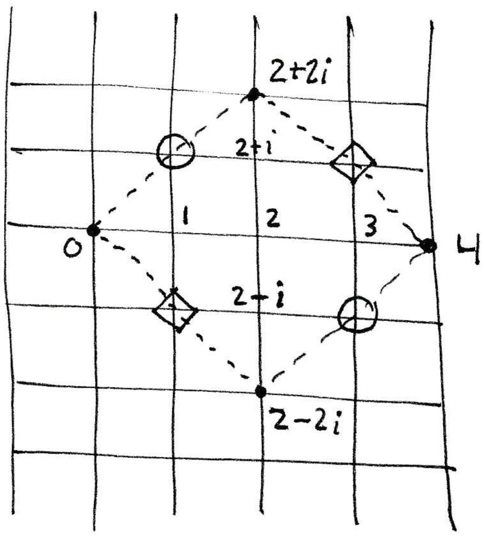
Notice $a=2$, $b=1+i$ gives $ab = 2(1+i) = 2+2i$

hence $ab \in \langle 2+2i \rangle$. However for $a, b \in \langle 2+2i \rangle$

we must solve $c(2+2i) = 2$ or $d(2+2i) = 1+i$

$$\Rightarrow \underbrace{c=1,\ c=0}_{\text{nonsense}} \quad \text{and} \quad \underbrace{d = 1/2}_{\text{not in } \mathbb{Z}.}$$

thus $a, b \notin \langle 2+2i \rangle$ which proves $\langle 2+2i \rangle$ not prime.



$2+2i$, $-2-2i$, $2i-2$, $2-2i$ all generate $\langle 2+2i \rangle$

O : $1+i + \langle 2+2i \rangle$
◇ : $1-i + \langle 2+2i \rangle$

Let $J = \langle 2+2i \rangle$

$$\boxed{\mathbb{Z}[i]/\langle 2+2i \rangle = \{ J,\ 1+i+J,\ 1-i+J,\ 1+J,\ 2+J,\ 3+J,\ 2+i+J,\ 2-i+J \} \quad \underline{8 \text{ elements}}}$$

$4 \cdot (1+J) = 4 + J = J$ and $1+J,\ 2+J,\ 3+J \neq J$

thus $\text{Char}\left(\mathbb{Z}[i]/\langle 2+2i \rangle \right) = 4$

(characteristic is # of times to add 1 to get 0)

$\boxed{P101}$ # 43 p. 262

Let R be commutative ring. Show $R/N(\langle 0 \rangle)$ has no nonzero nilpotent elements.

$$N(\langle 0 \rangle) = \{ r \in R \mid r^n \in \langle 0 \rangle \text{ for some } n \in \mathbb{N} \}$$

That is, $N(\langle 0 \rangle) = \{ r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{N} \}$.

Let $J = N(\langle 0 \rangle)$ then

$$R/N(\langle 0 \rangle) = \{ x + J \mid x \in R \}$$

Suppose $(x+J)^n = J$ for some $n \in \mathbb{N}$

then,

$$(x+J)^n = x^n + J = J \Rightarrow x^n \in J$$

therefore, $\exists m \in \mathbb{N}$ for which $(x^n)^m = 0$

and we find $x^{nm} = 0 \Rightarrow x \in J$

consequently $x + J = J$ which shows the only nilpotent element in $R/N(\langle 0 \rangle)$ is $N(\langle 0 \rangle)$.

(aka zero)

$\boxed{P102}$ # 47 p. 262

Show that $\mathbb{Z}_3[x]/\langle x^2+x+1\rangle$ is not a field

Notice $1^2+1+1 = 3 = 0$ in $\mathbb{Z}_3$ thus $(x-1) \mid x^2+x+1$.

$$\begin{array}{r|l} & x+2 \\ \hline x-1 & x^2+x+1 \\ & x^2-x \\ \hline & 2x+1 \\ & 2x-2 \\ \hline & 3=0. \end{array}$$

$\hookrightarrow x^2+x+1 = (x-1)(x+2)$

Thus $\underbrace{(x-1+\langle x^2+x+1\rangle)(x+2+\langle x^2+x+1\rangle)}_{\text{ZERO DIVISORS !}} = \underbrace{x^2+x+1+\langle x^2+x+1\rangle}_{\langle x^2+x+1\rangle}$

Thus $x-1+\langle x^2+x+1\rangle$ has no inverse. (multiplicative)

$\Rightarrow \mathbb{Z}_3[x]\big/\langle x^2+x+1\rangle$ is not a field.

Remark: this problem helps us see why irreducibility is so important. When $f(x) = g(x)h(x)$ then

$\dfrac{R[x]}{\langle f(x)\rangle}$ picks up $g(x)+\langle f(x)\rangle$ and $h(x)+\langle f(x)\rangle$ as zero-divisors.