SOLUTIONS TO LECTURE 24 PROBLEMS 91 – 96

P91 Gallian #16 from p. 247

A ring element a is called <u>idempotent</u> if $a^2 = a$. Prove the only idempotents of an integral domain are $a = 0, 1$

Let R be a commutative ring with unity 1 with no zero divisors. That is, suppose R is an integral domain. If $a = 0$ then $a^2 = (0)(0) = 0 = a$. If $a \neq 0$ then $a^2 = a = a(1)$ yields $a(a) = a(1)$ with $a \neq 0$ hence by CANCELLATION OF INTEGRAL DOMAINS, $\underline{a = 1}$. Thus $a^2 = a$ implies either $\boxed{a = 0}$ or $\boxed{a = 1}$ in $\int$-domain.

P92 Gallian #24 from pg. 247

Let $d > 0$, $d \in \mathbb{Z}$. Prove $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a field.

Observe $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{R}$ hence to show $\mathbb{Q}[\sqrt{d}]$ is subring of $\mathbb{R}$ we need only note $0 + 0\sqrt{d} = 0 \in \mathbb{Q}[\sqrt{d}]$ to see $\mathbb{Q}[\sqrt{d}] \neq \emptyset$. Also, $a + b\sqrt{d}$, $x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ then $(a + b\sqrt{d}) - (x + y\sqrt{d}) = (a - x) + (b - y)\sqrt{d}$ and as $a, b, x, y \in \mathbb{Q}$ it follows $a - x,\ b - y \in \mathbb{Q}$ hence, $(a + b\sqrt{d}) - (x + y\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$. Likewise,

$$\begin{aligned}(a + b\sqrt{d})(x + y\sqrt{d}) &= ax + ay\sqrt{d} + bx\sqrt{d} + by(\sqrt{d})^2 \\ &= ax + byd + (ay + bx)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]\end{aligned}$$

Thus $\mathbb{Q}[\sqrt{d}]$ forms a <u>ring</u>. Continued

P92 continued

$\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{R}$ is subring of commutative ring $\mathbb{R}$ thus $\mathbb{Q}[\sqrt{d}]$ is commutative ring. Moreover,

$1(a+b\sqrt{d}) = a+b\sqrt{d}$ and $1 = 1+0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$

thus $\mathbb{Q}[\sqrt{d}]$ is unital. Let $a+b\sqrt{d} \neq 0$

Note that $\left(\dfrac{a-b\sqrt{d}}{a^2-b^2d}\right)(a+b\sqrt{d}) = \dfrac{a^2-b^2d}{a^2-b^2d} = 1$

thus $(a+b\sqrt{d})^{-1} = \dfrac{a-b\sqrt{d}}{a^2-b^2d} \in \mathbb{Q}[\sqrt{d}] \Rightarrow \mathbb{Q}[\sqrt{d}]$ is a field.

① Remark: we should comment that

$\dfrac{a}{a^2-b^2d}, \dfrac{-b}{a^2-b^2d} \in \mathbb{Q}$ and we

know $a^2-b^2d \neq 0$ as to suppose otherwise gives $db^2 = a^2 \Rightarrow d = \dfrac{a^2}{b^2} \Rightarrow \sqrt{d} = \pm\dfrac{a}{b}$

But, $\sqrt{d} \notin \mathbb{Q}$ and $\pm\frac{a}{b} \in \mathbb{Q}$ is a $\rightarrow\leftarrow$

So we find $a^2-b^2d \neq 0$ for $d>0, d \in \mathbb{Z}$

– (assuming d is not a square!) –

---

② I should say at outset, if $d = m^2$ then $m>0$, $m \in \mathbb{Z}$

$a+b\sqrt{d} = a+b\sqrt{m^2} = a+bm \in \mathbb{Q}$, so we can show that $\mathbb{Q}[\sqrt{m^2}] = \mathbb{Q}$. We really want $d \neq m^2$.

$\boxed{P93}$ Gallian # 35 pg. 248

> the nonzero elements of $\mathbb{Z}_3[i]$ form an Abelian group of order 8 under multiplication. Is this group $\approx$ to $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$?

$1, 2, 1+i, 1+2i, 2+i, 2+2i, i, 2i$

are the 8 nonzero elements in $\mathbb{Z}_3[i]$

$$(2)(2) = 4 = 1$$

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

$$((1+i)(1+i))^2 = (2i)^2 = 4(-1) = -4 = 2 = (1+i)^4$$

$$(1+i)^8 = ((1+i)^4)^2 = (2)^2 = 4 = 1$$

Thus $1+i$ is an element of order 8 in $\mathbb{Z}_3[i]^\times$

thus $\boxed{U(\mathbb{Z}_3[i]) \approx \mathbb{Z}_8}$.

$\boxed{P94}$ Gallian # 34 pg. 262

> Prove $I = \langle 2+2i \rangle$ is not a prime ideal of $\mathbb{Z}[i]$
> How many elements are in $\mathbb{Z}[i]/I$

Consider, $(2 + \langle 2+2i \rangle)(1+i + \langle 2+2i \rangle) = 2+2i + \langle 2+2i \rangle$

thus $2 + \langle 2+2i \rangle$ is a zero divisor in $\mathbb{Z}[i]/I$

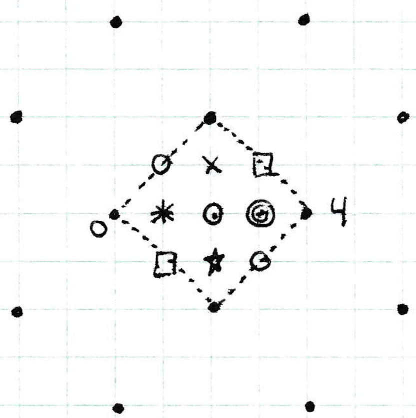
and hence $\mathbb{Z}[i]/I$ is not an integral domain and we deduce I is <u>not</u> a prime ideal. There are 8 elements in $\mathbb{Z}[i]/I$. I saw this graphically ↷

P94 continued

I draw

$$2+2i, \quad -2-2i, \quad 2i-2, \quad -2i+2$$

and sums of these to obtain graphical rep. of $I = \langle 2+2i \rangle$ in $\mathbb{Z}[i]$. Then identify fundamental region which gets repeated and simply count the distinct points modulo I,



The cosets are, $I = \langle 2+2i \rangle$,

$$\frac{\mathbb{Z}[i]}{I} = \{ \underbrace{I}_{\bullet}, \underbrace{1+i+I}_{\circ}, \underbrace{1-i+I}_{\square}, \underbrace{1+I}_{*}, \underbrace{2+I}_{\odot}, \underbrace{3+I}_{\circledcirc}, \underbrace{2+i+I}_{\times}, \underbrace{2-i+I}_{\star} \}$$

$\boxed{P95}$ $\boxed{\# 45}$ pg. 262

Show $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field

Let $f(x) = x^2 + x + 1$

Note $f(0) = 0 + 0 + 1 = 1 \neq 0$

and $f(1) = 1^2 + 1 + 1 = 1 \neq 0$

thus $f(x)$ has no zero in $\mathbb{Z}_2$ and hence no linear factor exists in $f(x) \Rightarrow f(x)$ is irreducible.

<u>FUTURE Sol$^{\underline{n}}$</u> : $\underbrace{\text{irreducible } f(x) \Rightarrow \langle f(x)\rangle \text{ maximal}}_{\text{Chapter 17 result. (Th}^{\underline{m}}\text{ 17.5)}} \Rightarrow \dfrac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ a field

At this stage we must show maximality of $\langle f(x)\rangle$ directly. Suppose $\langle x^2+x+1\rangle \subseteq I$ we need to show $I = \langle x^2+x+1\rangle$ or $I = \mathbb{Z}_2[x]$ to demonstrate maximality (we assume I is an ideal) <u>OR</u> we can show $\dfrac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ is a field directly (following Gallian's hint)

$\dfrac{\mathbb{Z}_2[x]}{I} = \{ I, 1+I, x+I, x+1+I \}$ as $x^2 + I = x+1+I$ allows us to reduce to these 4 cosets.

I serves as zero in $\mathbb{Z}_2[x]/I$,

$(1+I)(a+bx+I) = a+bx+I$ so $1+I$ serves as 1

Consider,

$(x+I)(x+1+I) = x^2+x+I = 1+I$ as $x^2+x-1 \in I$ as $x^2+x-1 = x^2+x+1$.

thus $(x+I)^{-1} = x+1+I$. Likewise, $(x+1+I)^{-1} = x+I$. We know $(1+I)(1+I) = 1+I$.

So every nonzero element in $\mathbb{Z}_2[x]/I$ has mult. inverse.

Moreover, $\mathbb{Z}_2[x]/I$ is commutative ring with unity $\therefore \mathbb{Z}_2[x]/I$ is a field.

P96 Prove Th^{m} 3.2.11

If R is commutative ring with identity and $a_1, a_2, \dots, a_n \in R$ then $\langle a_1, a_2, \dots, a_n \rangle$ is an ideal

<u>Proof:</u> we define for $a_1, a_2, \dots, a_n \in R$,

$$\langle a_1, a_2, \dots, a_n \rangle = \{ a_1 r_1 + a_2 r_2 + \cdots + a_n r_n \mid r_1, r_2, \dots, r_n \in R \}$$

Suppose $x, y \in \langle a_1, a_2, \dots, a_n \rangle$ then $\exists r_i, s_i \in R$ for which $x = a_1 r_1 + \cdots + a_n r_n$ and $y = a_1 s_1 + \cdots + a_n s_n$ then

$$\begin{aligned} y - x &= (a_1 s_1 + \cdots + a_n s_n) - (a_1 r_1 + \cdots + a_n r_n) \\ &= a_1 (s_1 - r_1) + \cdots + a_n (s_n - r_n) \in \langle a_1, a_2, \dots, a_n \rangle. \end{aligned}$$

Also, if $r \in R$ then

$$\begin{aligned} xr &= (a_1 r_1 + \cdots + a_n r_n) r \\ &= a_1 (r_1 r) + \cdots + a_n (r_n r) \in \langle a_1, a_2, \dots, a_n \rangle \end{aligned}$$

thus $\langle a_1, a_2, \dots, a_n \rangle$ forms an ideal of R.