Solution to Lecture 29 Problems 121 – 126

P121 find $\gcd(\alpha, \beta)$ for $\alpha = 12+3i$, $\beta = 6-9i$

$$(\alpha, \beta) = (12+3i,\ 6-9i)$$

$$(6-9i,\ 3-3i) = (\beta,\ \alpha - i\beta)$$

$$\begin{array}{r} 6-9i \\ -6+6i \\ \hline -3i \end{array}$$

$$(3-3i,\ -3i) = (\alpha - i\beta,\ \beta - 2(\alpha - i\beta))$$

$(\beta - 3i) = -2i(1-i)$

$$(-3i,\ 0) = (\beta - 2(\alpha - i\beta),\ \alpha - i\beta + (1+i)(\beta - 2(\alpha - i\beta)))$$

not needed I'm just playing around here.

$$0 = \alpha - i\beta - (1+i)((1+2i)\beta - 2\alpha)$$

$$0 = \alpha - i\beta - (1+i+2i-2)\beta + 2(1+i)\alpha$$

$$0 = \alpha - i\beta - (-1+3i)\beta + 2\alpha + 2i\alpha$$

$$0 = (3+2i)\underbrace{(12+3i)}_{\alpha} + (1-4i)\underbrace{(6-9i)}_{\beta}$$

$$0 = 3(3+2i)(4+i) + 3(1-4i)(2-3i)$$

– (just curious, not needed) –

The last nonzero remainder shows $\boxed{\gcd(\alpha, \beta) = -3i}$ (could say $\pm 3, \pm 3i$ here)

and $\quad -3i = \beta - 2(\alpha - i\beta)$

$$-3i = -2\alpha + (1+2i)\beta \quad \curvearrowright \text{multiply by } i$$

$$\underline{3 = -2i\alpha + (i-2)\beta}.$$

Notice, $N(\pm 3) = N(\pm 3i) = 9$, this is the greatest norm of a common divisor to $\alpha = 12+3i$ and $\beta = 6-9i$. This follows from the Euclidean Algorithm guided by $N: \mathbb{Z}[i] \to \mathbb{Z}$.

P122 #10 on p. 325 Gallian

Let D be a PID and $p \in D$. Prove $\langle p \rangle$ is maximal ideal $\iff$ p is irreducible.

Let D be a PID and $p \in D$.

$\Rightarrow$ Assume $\langle p \rangle = \{pr \mid r \in D\}$ is a maximal ideal.

Suppose $p = xy$ for $x, y \in D$ then for each $r \in R$,

$$pr = x(yr) \in \langle x \rangle$$

thus $\langle p \rangle \subseteq \langle x \rangle \subseteq D$. By maximality, we find $\langle p \rangle = \langle x \rangle$ or $\langle x \rangle = D$. Consider,

(1.) if $\langle p \rangle = \langle x \rangle$ thus $x = pr'$ for some $r' \in D$ and hence $p = xy = pr'y \Rightarrow r'y = 1$ $\therefore$ y is unit

recall D a PID means D is an integral domain where every ideal is principal. Thus $p = p(1) = p(r'y) \Rightarrow 1 = r'y$ by cancellation.

(2.) if $\langle x \rangle = D$ then $\exists r' \in D$ such that $xr' = 1$ $\therefore$ x unit thus x is a unit.

In any event we find $p = xy \Rightarrow$ x a unit or y a unit thus p is irred in D.

$\Leftarrow$ Assume p is irreducible. Consider $\langle p \rangle \subseteq I \subseteq D$ since D is PID $\Rightarrow$ $I = \langle x \rangle$ for some $x \in D$.

$p \in \langle p \rangle \subseteq \langle x \rangle \Rightarrow p = xr$ for some $r \in D$.

Thus x is a unit (in which case $\langle x \rangle = D$ $\therefore$ $I = D$) or r is a unit (in which case $\langle p \rangle = \langle x \rangle$ $\therefore$ $I = \langle p \rangle$) by the irreducibility of p. Hence $\langle p \rangle$ is maximal as $\langle p \rangle \subseteq I \subseteq D \Rightarrow I = \langle p \rangle$ or $I = D$.

P123 #14 of p. 325 Gallian

Show $1-i$ is an irred. in $\mathbb{Z}[i]$

If $1-i = xy$ then $N(1-i) = N(xy) = N(x)N(y)$

where $N(a+ib) = a^2+b^2$ defines the usual norm in $\mathbb{Z}[i]$.

Thus $2 = N(x)N(y) \Rightarrow N(x)=1$ or $N(y)=1$

$\Rightarrow$ x a unit or y a unit

$\Rightarrow$ $1-i$ is irred. in $\mathbb{Z}[i]$.

P124 #19 of p. 326 Gallian

Prove: if p is a prime which has form $p = a^2+b^2$ then $a+bi$ is irreducible in $\mathbb{Z}[i]$. Find three primes that have this property and find the corresponding irreducibles in $\mathbb{Z}[i]$

Suppose p is prime and $\exists a,b \in \mathbb{Z}$ s.t. $p = a^2+b^2$

then $N(a+bi) = a^2+b^2 = p$ thus $a+bi = xy$

implies $N(a+bi) = N(x)N(y) \Rightarrow p = N(x)N(y)$

thus $N(x)=1$ or $N(y)=1 \Rightarrow$ x a unit or y a unit

Hence $a+ib$ is an irreducible in $\mathbb{Z}[i]$.

//

There are many possible answers! But, this interplay between primes and $\mathbb{Z}[i]$ is one of the reasons $\mathbb{Z}[i]$ is neat,

$5 = 1^2+2^2$ has corresponding irred. $1\pm 2i$ and $-1\pm 2i$.

$13 = 2^2+3^2$ has corr. irreds $2\pm 3i$ and $-2\pm 3i$.

$17 = 1^2+4^2$ has corres. irreds $1\pm 4i$, $-1\pm 4i$.

P125 # 7 from p. 331 of Gallian

Prove $I[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_0, a_1, \ldots, a_n \in 2\mathbb{Z} \}$ forms a prime ideal in $\mathbb{Z}[x]$

Suppose $a(x), b(x) \in \mathbb{Z}[x]$ and $a(x)\,b(x) \in I[x]$ to show $a(x) \in I[x]$ or $b(x) \in I[x]$ seems rather much trouble, we should try some indirect argument to show $I[x]$ is prime ideal.

//

Notice $I = 2\mathbb{Z} = \langle 2 \rangle$ is prime ideal of $\mathbb{Z}$ as

$xy \in \langle 2 \rangle \Rightarrow xy = 2k \Rightarrow x$ or y is in $2\mathbb{Z}$.

Moreover, $I[x] = (2\mathbb{Z})\mathbb{Z}[x] = (2\mathbb{Z})[x]$ and,

by # 38 from p. 292 of Gallian (aka our P110)

we find

$I = 2\mathbb{Z}$ prime ideal of $\mathbb{Z}$ $\Rightarrow$ $I[x] = (2\mathbb{Z})[x]$ prime ideal of $\mathbb{Z}[x]$.

//

To give a stand-alone argument, let

$$\psi(a_n x^n + \cdots + a_1 x + a_0) = (a_n + 2\mathbb{Z})x^n + \cdots + (a_1 + 2\mathbb{Z})x + a_0 + 2\mathbb{Z}$$

define a ring homomorphism from $\mathbb{Z}[x] \longrightarrow (\mathbb{Z}/2\mathbb{Z})[x]$.

Observe ψ is a surjection and

$$\ker \psi = (2\mathbb{Z})[x]$$

thus $\mathbb{Z}[x]/2\mathbb{Z}[x] \cong (\mathbb{Z}/2\mathbb{Z})[x]$ by 1st iso. Thm of rings.

Note, $\mathbb{Z}/2\mathbb{Z}$ a field $\Rightarrow (\mathbb{Z}/2\mathbb{Z})[x]$ is an integral domain

and so $\dfrac{\mathbb{Z}[x]}{2\mathbb{Z}[x]} \cong \left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)[x] \Rightarrow 2\mathbb{Z}[x]$ is a prime ideal.

P126 # 24 of p. 332 in Gallian

Express both 13 and $5+i$ as products of irreducibles in $\mathbb{Z}[i]$

Notice $N(13) = 169 = 13^2 \Rightarrow$ need $N(a+ib) = 13$ for factorization, $a+ib = 2 \pm 3i$ do nicely and

$$\boxed{(2+3i)(2-3i) = 13}$$

Observe $N(2 \pm 3i) = 4 + 9 = 13$ hence only

$$2 \pm 3i = xy \Rightarrow 13 = N(x)N(y)$$
$$\Rightarrow N(x) = 1 \text{ or } N(y) = 1$$
$$\Rightarrow \underline{x \text{ a unit}} \text{ or } \underline{y \text{ a unit}}$$
$$\Rightarrow 2 \pm 3i \text{ are irred.}$$

On the other hand,

$$N(5+i) = 25 + 1 = 26 = 2(13)$$

suggests a reduction of $5+i = xy$ where $\underbrace{N(x) = 2}_{x = 1-i}$ and $\underbrace{N(y) = 13}_{y = 2+3i}$

these are both irreducible for essentially the same reason.

Note, $(1-i)(2+3i) = 2 - 2i + 3i - 3i^2 = 5 + i$

thus $\boxed{5+i = (1-i)(2+3i)}$

- (deciding on $1-i$ vs. $-1 \pm i$ or $1+i$ & $2+3i$ vs. $-2 \pm 3i$ or $2-3i$ took me a few minutes of tinkering) -