SOLUTIONS TO LECTURE 28 PROBLEMS 115 – 120

P115 Let d be squarefree and $N(a+b\sqrt{d}) = |a^2 - b^2 d|$ for $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Let $x = a + b\sqrt{d}$,

$$N(x) = 0 \Rightarrow |a^2 - b^2 d| = 0$$
$$\Rightarrow a^2 - b^2 d = 0$$
$$\Rightarrow a^2 = b^2 d$$
$$\Rightarrow \frac{a^2}{b^2} = d \quad \text{or} \quad b = 0 \text{ and } a = 0.$$
$$\Rightarrow \underbrace{\pm\frac{a}{b} = \sqrt{d}}_{\text{impossible as } \pm\frac{a}{b} \in \mathbb{Q} \text{ whereas } \sqrt{d} \notin \mathbb{Q}} \quad \text{or} \quad \underbrace{a = b = 0}_{\text{means } x = 0}$$

Conversely, $x = 0 = 0 + 0\sqrt{d}$ has $N(x) = 0$. Thus,

$$N(x) = 0 \iff x = 0.$$

P116 Let $x = a + b\sqrt{d}$, $y = u + v\sqrt{d}$ hence

$$xy = (a + b\sqrt{d})(u + v\sqrt{d}) = au + dbv + (av + bu)\sqrt{d}$$

Hence, $N(xy) = |(au + dbv)^2 - (av + bu)^2 d|$

$$= |a^2u^2 + \cancel{2audbv} + d^2b^2v^2 - (a^2v^2 + \cancel{2avbu} + b^2u^2)d|$$
$$= |a^2(u^2 - v^2d) - b^2d(u^2 - v^2d)|$$
$$= |(a^2 - b^2d)(u^2 - v^2d)|$$
$$= |a^2 - b^2d|\,|u^2 - v^2d|$$
$$= N(x)N(y). \;//$$

P117 Gallian #14 p. 308

Let $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$

Write $f(x)$ as product of irred. poly. in $\mathbb{Z}_2[x]$.

$$\begin{aligned} f(x) &= x^2(x+1) + x+1 \\ &= (x^2+1)(x+1) \\ &= (x^2-1)(x+1) \\ &= (x+1)^2(x-1) \\ &= \underline{(x+1)^3}. \end{aligned}$$

P118 #4 of p. 325 Gallian

Let D be an integral domain. Suppose $a \in D$ is an irreducible and $u \in D$ is a unit. Consider $b = au$

if $b = b_1 b_2$ then $au = b_1 b_2 \Rightarrow a = b_1 b_2 u^{-1}$

thus $a = b_1 b_2'$ where $b_2' = b_2 u^{-1}$. Since a is irred. we find b_1 or b_2' is a unit $v \in D$ hence

$b = b_1 b_2$ has b_1 a unit if b_1 is unit

and if $b_2' = v = b_2 u^{-1} \Rightarrow b_2 = uv$ which is a unit as $U(D)$ forms a group (indeed $(uv)^{-1} = v^{-1}u^{-1}$). Thus, in every case, we find $b = b_1 b_2$ has b_1 or b_2 a unit. Thus b is irred.

Remark: you might find a $\not\rightarrow$ natural here as well...

P119 #17 of p. 326 Gallian

In $\mathbb{Z}[i]$ show 3 is irred, but 2 and 5 are not.

Recall $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, $N(\pm 1) = N(\pm i) = 1$

If $3 = xy$ for some $x, y \in \mathbb{Z}[i]$ then

$N[a+ib] = a^2 + b^2$ provides, as $N[a+ib] \in \mathbb{Z}$,

$$N(3) = N(x)\,N(y)$$

$$9 = N(x)\,N(y) \Rightarrow \underline{N(x) = N(y) = 3} \quad \text{or} \quad \begin{matrix} N(x) = 9 \\ N(y) = 1 \end{matrix} \quad \text{or} \quad \begin{matrix} N(x) = 1 \\ N(y) = 9 \end{matrix}$$

$a^2 + b^2 = 3$ has no $\mathbb{Z}$-sol'ns

Thus $N(x) = 1$ or $N(y) = 1$ for $3 = xy$ which means x or y is a unit hence $\underline{3 \in \mathbb{Z}[i] \text{ is irred.}}$

In contrast, $2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$ ← show 2 & 5 are reducible in $\mathbb{Z}[i]$.

P120 #18 from p. 326

Prove 7 is irred. in $\mathbb{Z}[\sqrt{6}]$ even though $N(7)$ not prime

Let $N(a + b\sqrt{6}) = |a^2 - 6b^2|$. Notice $a^2 - 6b^2 = \pm 1$ provides $a = \pm 1$, $b = 0$ as sol'ns. $\therefore$ $U = \pm 1$ units. also, $a = \pm 5$, $b = \pm 2$ give $\pm 5 \pm 2\sqrt{6}$ as units... there may be more... In any event, suppose $7 = xy$ and notice

$$N(7) = 49 = N(x)N(y)$$

either 7 is irreducible or $N(x) = N(y) = 7$. Suppose, $\exists\, a, b, u, v \in \mathbb{Z}$ s.t. $x = a + b\sqrt{6}$, $y = u + v\sqrt{6}$ and $a^2 - 6b^2 = \pm 7$ and $u^2 - 6v^2 = \pm 7$. Note,

↓

P120 continued

$a^2 - 6b^2 = \pm 7 \Rightarrow \underline{a^2 - 6b^2 = 0} \mod 7$

We can check $a = \pm 1, \pm 2, \pm 3$ do not provide sol^{n}'s

$\underline{a = \pm 1}$ $1 - 6b^2 = \begin{cases} 1 & b = 0 \\ -5 & b = \pm 1 \\ -23 & b = \pm 2 \\ -53 & b = \pm 3 \end{cases}$

$\underline{a = \pm 2}$ $4 - 6b^2 = \begin{cases} 4 & b = 0 \\ -2 & b = \pm 1 \\ -20 & b = \pm 2 \\ -50 & b = \pm 3 \end{cases}$

$\underline{a = \pm 3}$ $9 - 6b^2 = \begin{cases} 9 & b = 0 \\ 3 & b = \pm 1 \\ -15 & b = \pm 2 \\ -45 & b = \pm 3 \end{cases}$

thus $a = b = 0$ is only mod 7 sol^{n} of $a^2 - 6b^2 = 0$

consequently $N(x) = N(a + b\sqrt{6}) = a^2 - 6b^2 = 7$

implies $a \equiv 0$ and $b \equiv 0 \mod 7$, but

$7 \mid a$, $7 \mid b \Rightarrow 49 \mid (a^2 - 6b^2) \Rightarrow 49 \mid 7$ impossible!

$\therefore$ $N(x) = 7$ is not possible.

$\therefore$ $7 = xy \Rightarrow x$ or y a unit.

i.e. 7 is irred. in $\mathbb{Z}[\sqrt{6}]$.

– (I hope you see I'm just borrowing the concept of Example 2 on p. 313) –