Homework 10, selected solutions

DF 8.3 #5a. Suppose $2 = (a+b\sqrt{-n})(c+d\sqrt{-n})$

Then $4 = N(2) = N(a+b\sqrt{-n})\,N(c+d\sqrt{-n})$

$\Rightarrow \quad 4 = (a^2+nb^2)(c^2+nd^2)$ since $n>3$,

if $b^2 \neq 0$, then $b^2 = 1$ and $n = 4$, in which case $N(a+b\sqrt{-n}) = 4$

so $N(c+d\sqrt{-n}) = 1$ so it is a unit.

Similarly, if $d \neq 0$, then $a+b\sqrt{-n}$ is a unit.

So $b = d = 0$, But 2 is irreducible in $\mathbb{Z}$.

Suppose $\sqrt{-n} = (a+b\sqrt{-n})(c+d\sqrt{-n})$

As before $N(0+\sqrt{-n}) = 1^2 n = n = N(a+b\sqrt{-n})\,N(c+d\sqrt{-n})$

$= (a^2+nb^2)(c^2+nd^2)$

If $b^2 \neq 0$ then $a^2+nb^2 > n$ unless $b = 1$ and $a = 0$.

so $n = (0+n\cdot 1^2)(c^2+nd^2) \Rightarrow c^2+nd^2 = 1$

$\Rightarrow c = 0 \quad d^2 = 1$ so $c+d\sqrt{-n}$ is a unit.

Similarly, If $d^2 \neq 0$, then $a+b\sqrt{-n}$ is a unit.

So we are left with the case $b^2 = 0 \neq d^2 = 0$

This means that $\sqrt{-n} = ac \in \mathbb{Z}$ but $\sqrt{-n} \notin \mathbb{Z}$.

2. One possible answer:

By problem 1, $\sqrt{-6}$ is irreducible in $\mathbb{Z}[\sqrt{-6}]$.

Then $-6 = \sqrt{-6}\cdot\sqrt{-6}$ is a factorization into irreducibles

But $-6 = 2\cdot(-3)$ is another factorization. 2 is irreducible by problem 1 and -3 is irreducible as well (by a similar argument)

3 a) Let F be a field.

Then $F[x]$ is a Euclidean domain, hence a UFD.

$x^2-1 = (x-1)(x+1)$. Both $x-1$ and $x+1$ are irreducible, since if a degree 1 polynomial is a product $p(x)\,q(x)$, then one of $p(x)$ or $q(x)$ is degree 0, so a unit in $F[x]$.

This shows that $x^2-1 = (x-1)(x+1)$ is the unique factorization of x^2-1 into irreducibles.

We saw in class that if $a \in F$ is a root of x^2-1 then $(x-a)$ is a factor of x^2-1. Thus, the only solutions of $x^2-1=0$ are $x=1$ and $x=-1$.

b) Let p be prime $\mathbb{Z}/p\mathbb{Z}$ is a field. Look at the polynomial x^2-1 in $\mathbb{Z}/p\mathbb{Z}[x]$. By part a, the only roots of this polynomial in $\mathbb{Z}/p\mathbb{Z}$ are $x=1$ and $x=-1$. So if $x^2=1$ in $\mathbb{Z}/p\mathbb{Z}$, either $x=1$ or $x=-1$

But $x^2=1$ is equivalent to $x=x^{-1}$.

Therefore the only integers that are their own inverse mod p are those congruent to 1 or -1 mod p.

c) $(a!)^2 = 1\cdot 2\cdot 3 \cdots (2a-1)\cdot 2a \cdot 1\cdot 2\cdot 3 \cdots (2a-1)\cdot 2a$

Since for any n, $n \equiv -p+n \bmod p$, this is congruent to

$$1\cdot 2\cdot \cdots (2a-1)\cdot 2a \cdot (1-p)\cdot(2-p)\cdots(2a-p) \quad \bmod p$$

$$= 1\cdot 2 \cdots (2a-1)\cdot 2a \cdot (-2a+1))\,(-(2a-2)) \cdots (-(p-1)) \qquad \text{since } 4a+1 = p \text{ so } 2a = p-2a-1$$

$$= (-1)^{2a}\, 1\cdot 2\cdot 3\cdot \cdots \cdot (p-1)$$

In $\mathbb{Z}/p\mathbb{Z}$, each element cancels with its (unique, different) multiplicative inverse (no element is its own inverse except 1 and $p-1$) except for 1 and $p-1$

Thus $((2a)!)^2 \equiv p-1 \bmod p$

$\Rightarrow$ $(2a)!^2 + 1 \equiv 0 \bmod p$, so p divides $(2a)!^2+1$

5 b.) Let $f(x) \in \mathbb{R}[x]$, and write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

If $f(\alpha) = 0$, this means

$$a_n(\alpha^n) + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0 \quad \text{in } \mathbb{C}$$

Apply ϕ. Since $\phi(0) = 0$ and ϕ is a ring homomorphism,

$$\phi(a_n)\,\phi(\alpha)^n + \phi(a_{n-1})\,\phi(\alpha)^{n-1} + \dots + \phi(a_1)\,\phi(\alpha) + \phi(a_0) = 0$$

Since $a_i \in \mathbb{R}$, $\phi(a_i) = a_i$.

It follows that $a_n\,\phi(\alpha)^n + \dots + a_1\,\phi(\alpha) + a_0 = 0$

in other words $f(\phi(\alpha)) = 0$.

c) Suppose $f \in \mathbb{R}[x]$ has degree at least 2, and f is irreducible.

We'll show that f has to have degree 2.

Let $\alpha \in \mathbb{C}$ be a root, so $f(\alpha) = 0$. By part b, $f(\phi(\alpha)) = 0$.

so $\phi(\alpha)$ is also a root. Write $\alpha = a + bi$ $\phi(\alpha) = a - bi$

Then $(x - (a+bi))$ and $(x - (a-bi))$ both divide f, consider

their product $g(x) = (x - (a+bi))(x - (a-bi)) = (x^2 + (a^2+b^2))$

We claim that $g(x)$ divides f

To show this, divide f by g, using the division algorithm

$$f(x) = q(x)\,g(x) + r(x) \quad \text{where} \quad \deg r(x) < 2.$$

But, since $f(\alpha) = 0$ and $g(\alpha) = 0$

we have $r(\alpha) = 0$, and since $f(\phi(\alpha)) = 0$ and $g(\phi(\alpha)) = 0$

$r(\phi(\alpha)) = 0$.

But then r has two roots, so degree ≥ 2, a contradiction.

Since f is irreducible, $f(x) = g(x) \cdot c$ for some unit c, i.e.

a degree 0 polynomial.

Thus, f has degree 2.