MATH 611 HW5 SOLUTIONS

Friday 12/13/19.

2. $\omega = \frac{1}{2}(-1+\sqrt{-3})$, $\omega^3 = 1$.

$R = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Define $\sigma : R \longrightarrow \mathbb{Z}_{\geq 0}$

$$\sigma(a+b\omega) := \underbrace{|a+b\omega|^2}_{\therefore \geq 0} = (a+b\omega)(a+b\bar{\omega})$$

$$= a^2 + ab(\omega+\bar{\omega}) + b^2\omega\bar{\omega} = \underbrace{a^2 - ab + b^2}_{\therefore \in \mathbb{Z}}$$

Claim: R is a Euclidean domain with size function σ.

Proof: Given $\alpha, \beta \in R$, $\beta \neq 0$, required to prove $\exists\ q, r \in R$ s.t.

$\alpha = q \cdot \beta + r$ where $r = 0$ OR $\sigma(r) < \sigma(\beta)$.

$\alpha/\beta \in \mathrm{ff}\, R = \mathbb{Q}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$

$\left(\text{because } \frac{1}{a+b\omega} = \frac{a+b\bar{\omega}}{|a+b\omega|^2} = \frac{a+b\cdot(-1-\omega)}{a^2-ab+b^2} \in \mathbb{Q}[\omega].\right)$

Write $\alpha/\beta = a + b\omega$ $\quad a, b \in \mathbb{Q}$

$q = a' + b'\omega$ $\quad a', b' \in \mathbb{Z}$, $\quad |a'-a|, |b'-b| \leq 1/2$.

Then ~~$\alpha/\beta = q + r$ $\quad r = (a-a') + (b-b')\omega$~~

~~$\alpha = q \cdot (\beta + (a'-a)\omega + (b$~~

$\alpha/\beta = q + \underbrace{(a-a') + (b-b')\omega}_{\substack{\parallel \\ s = a'' + b''\cdot\omega,\ a'', b'' \in \mathbb{Q},\ |a''|, |b''| \leq 1/2}}$, $\quad |s|^2 = a''^2 - a''b'' + b''^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 3/4$ †

$\rightsquigarrow$ $\alpha = q \cdot \beta + r$, $r = s \cdot \beta$, $\sigma(r) = |r|^2 = |s|^2 \cdot |\beta|^2 \underset{\dagger}{\leq} 3/4 \cdot \sigma(\beta) < \sigma(\beta)$

□.

Now $ED \Rightarrow PID \Rightarrow UFD$.

So R is a UFD.

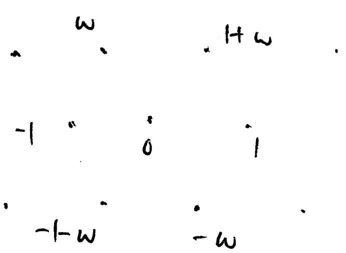
$\alpha \in R$ is a unit $\overset{\text{def}}{\Longleftrightarrow}$ $\exists\ \beta \in R$ s.t. $\alpha \cdot \beta = 1$.

$$\Rightarrow \quad \sigma(\alpha)\cdot\sigma(\beta) = 1 \qquad (\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta))$$

$$\Rightarrow \quad \sigma(\alpha) = 1 \qquad (\sigma(\alpha), \sigma(\beta) \in \mathbb{Z}_{\geq 0})$$

Conversely, if $\sigma(\alpha) = 1$, then $\alpha^{-1} = \dfrac{\bar{\alpha}}{|\alpha|^2} = \dfrac{\bar{\alpha}}{\sigma(\alpha)} = \bar{\alpha} \in R$.

So $\alpha \in R$ is a unit $\Leftrightarrow \sigma(\alpha) = 1$.



$\rightsquigarrow \quad R^{\times} = \{\pm 1, \pm\omega, \pm(1+\omega)\}$

4. We follow the hint

$$N: R \longrightarrow \mathbb{Z}_{\geq 0}$$

$$N(\alpha) := \alpha\bar{\alpha} = |\alpha|^2$$

ie $N(a+b\sqrt{-n}) = (a+b\sqrt{-n})(a-b\sqrt{-n}) = a^2+nb^2$

<u>Claim</u>: 2 is irreducible.

<u>Proof</u>: $N(2) = 2^2 = 4$.

$N(\alpha\beta) = N(\alpha)\cdot N(\beta)$. Similarly to Q2 above, α is a unit $\Leftrightarrow N(\alpha) = 1$.

So, if $2 = \alpha\cdot\beta$, α, β not units, then $4 = N(2) = N(\alpha)\cdot N(\beta)$, $N(\alpha), N(\beta) \neq 1$

$\Rightarrow N(\alpha) = N(\beta) = 2$.

But $a^2+nb^2 = 2$ has no solutions $a, b \in \mathbb{Z}$ for $n \geq 2$ #. $\therefore$ 2 is irred. $\square$.

Now we show R is not a UFD.

If n is even, $n = 2m$, then $n = 2 \cdot m = \sqrt{-n} \cdot -\sqrt{-n}$.

2 irred, $2 \nmid \pm\sqrt{-n}$ in R $\Rightarrow$ R not a UFD.

(recall: in a UFD, p irreducible $\Rightarrow$ p prime, i.e., $p | ab \Rightarrow p | a$ or $p | b$.)

If n is odd, $\overset{n = 2m-1}{|}$, $2m = n+1 = (1+\sqrt{-n})(1-\sqrt{-n})$.

2 irred, $2 \nmid 1 \pm \sqrt{-n}$ in R $\Rightarrow$ R not a UFD. $\square$.

5\. a. Required to prove $\quad \theta(\alpha+\beta) = \theta(\alpha) + \theta(\beta)$

$\quad\quad \& \ \theta(\alpha\beta) = \theta(\alpha) \cdot \theta(\beta)$

$\quad\quad \& \ \theta(1) = 1$.

These are easy to check. e.g. $\theta((a+b\sqrt{2})(c+d\sqrt{2})) = \theta((ac+2bd) + (ad+bc)\sqrt{2})$

$= (ac+2bd) - (ad+bc)\sqrt{2}$

$\theta(a+b\sqrt{2})\,\theta(c+d\sqrt{2}) = (a-b\sqrt{2}) \cdot (c-d\sqrt{2})$ // ✓

$= ac + 2bd - (ad+bc)\sqrt{2}$.

b. Now $\sigma(\alpha\beta) = |\alpha\beta \cdot \theta(\alpha\beta)| = |\alpha\beta \cdot \theta(\alpha) \cdot \theta(\beta)| = |\alpha \cdot \theta(\alpha)| \cdot |\beta \cdot \theta(\beta)|$

$= \sigma(\alpha) \cdot \sigma(\beta)$ ✓. $\square$.

$\sigma(\alpha) = \sigma(a+b\sqrt{2}) = |(a+b\sqrt{2})(a-b\sqrt{2})| = |a^2 - 2b^2|$

$\sigma(\alpha) = 0 \iff a^2 = 2b^2 \iff \pm a/b = \sqrt{2}$ or $(a,b) = (0,0)$.

But $\sqrt{2}$ is irrational, so $\sigma(\alpha) = 0 \iff \alpha = 0$. $\square$.

c. Similar to Q1. α unit $\Rightarrow \alpha \cdot \beta = 1$, some $\beta \in R$ $\Rightarrow \sigma(\alpha) \cdot \sigma(\beta) = 1 \Rightarrow \sigma(\alpha) = 1$

$\sigma(\alpha) = 1 \Rightarrow \alpha \cdot \beta = 1$, $\beta = \frac{\theta(\alpha)}{\sigma(\alpha)} = \theta(\alpha) \in R \Rightarrow \alpha$ unit. $\square$

d. $\sigma(1+\sqrt{2}) = |1^2 - 2\cdot 1^2| = |-1| = 1.$

$\Rightarrow$ $1+\sqrt{2}$ is a unit (with inverse $-1+\sqrt{2}$).

Now $(1+\sqrt{2})^n$ is a unit for all $n \in \mathbb{Z}$

(and these elements are distinct because $|1+\sqrt{2}| \neq 1$)

e. We show R is an ED w/ size function σ.

$\mathrm{Ff}\,R = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. We extend $\sigma : R \to \mathbb{Z}_{\geq 0}$ to $\sigma : \mathrm{Ff}\,R \to \mathbb{Q}_{\geq 0}$ by the same formula.

Given $\alpha, \beta \in R$, $\beta \neq 0$, $\alpha/\beta = a+b\sqrt{2}$ $a,b \in \mathbb{Q}$

$q := a'+b'\sqrt{2} \in R$, $a',b' \in \mathbb{Z}$, $|a'-a| \leq 1/2$, $|b'-b| \leq 1/2$.

$\leadsto$ $\alpha = q\cdot\beta + r$, $r \in R$, $\sigma(r) = \sigma(\beta)\cdot\sigma((a'-a)+(b'-b)\cdot\sqrt{2})$

$\leq \sigma(\beta)\cdot\left((1/2)^2 + 2\cdot(1/2)^2\right) = 3/4\,\sigma(\beta) < \sigma(\beta)$ □

Now ED $\Rightarrow$ PID $\Rightarrow$ UFD, so R is a UFD. □.

8. a. $f = x^3 + 4x + 1. \in \mathbb{Q}[x]$

f is a cubic, so f is irred $\Leftrightarrow$ f has no roots in $\mathbb{Q}$

If $a/b \in \mathbb{Q}$ is a root of $f = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, then $a \mid a_0$ & $b \mid a_n$.
$\gcd(a,b)=1$

So in our case possible roots $\alpha \in \mathbb{Q}$ are ± 1. $f(1) = 6 \neq 0$, $f(-1) = -4 \neq 0$.

So f is irreducible.

b. $x^4 + 10x^2 + 9 = (x^2+1)(x^2+9)$

irred because deg 2, & no roots in $\mathbb{Q}$.

c. $$x^6-1 = (x^3-1)(x^3+1)$$
$$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)$$

irred b/c deg 2 & no roots in $\mathbb{Q}$.

d. $x^4+3x^3+5x^2+x+7 \in \mathbb{Z}[x]$.

Reduce mod 2 $\rightsquigarrow$ $x^4+x^3+x^2+x+1 \in \mathbb{Z}/2\mathbb{Z}[x]$.

This is irred (by Q7).

So $x^4+3x^3+5x^2+x+7 \in \mathbb{Q}[x]$ is irred.

(We are using assertion proved in class: $f \in \mathbb{Z}[x]$, p prime, $p \nmid$ leading coeff of f, $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ irred, $\Rightarrow$ $f \in \mathbb{Q}[x]$ irred.)

e. $f = x^n+57$. $57 = 3 \cdot 19$.

So f irred by Eisenstein's criterion for $p=3$.

9. If f were reducible in $\mathbb{Q}[x]$, then $f = f_1 \cdots f_k$ where the f_i ~~are~~ irred in $\mathbb{Q}[x]$, $k>1$, $\deg f = \sum \deg f_i$. Moreover, WMA $f_i \in \mathbb{Z}[x]$ $\forall i$ by the Gauss Lemma.

Now, reducing mod p $\bar{f} = \bar{f}_1 \cdots \bar{f}_k$ (& note $\deg \bar{f} = \deg f$, $\deg \bar{f}_i = \deg f_i$ b/c p does not divide the lead coeffs)

The $\bar{f}_i$ may not be irred ~~anymore~~ in $\mathbb{Z}/p\mathbb{Z}[x]$, but we can factor them into irreds, obtaining the irred factorization of $\bar{f}$ as the product.

So, if f has an irred factor of deg d, then there are irred factors of $\bar{f}$ of degrees $d_1, \dots, d_l$ for some l

such that $d = d_1 + \dots + d_\ell$.

Now looking at the given irred factorizations of $\bar{f}$ for $p = 2, 3, 5, 7, 11$,

we see $d \neq 1$ $(p=7)$, $d \neq 2$ $(p=11)$, $d \neq 3$ $(p=11)$.

So f is irred in $\mathbb{Q}[x]$.

(Note: if f is reducible, $\exists$ irred factor g s.t. $\deg g \leq \frac{1}{2} \cdot \deg f$) $\square$.

10. a) $f = x^n + y^n - 1 \in \mathbb{C}[x,y] = (\mathbb{C}[y])[x]$

$\mathbb{C}(y) := \text{ff } \mathbb{C}[y]$

$y-1 \mid y^n - 1$, $(y-1)^2 \nmid (y^n - 1)$ $\Rightarrow f$ irred in $\mathbb{C}(y)[x]$

by generalized Eisenstein criterion, $p = y - 1$
$\quad \in \mathbb{C}[y]$

$\Rightarrow f$ irred in $(\mathbb{C}[y])[x] = \mathbb{C}[x,y]$ because primitive ($\gcd(\text{coeffts}) = 1$) $\square$.

b) $f = x^n y + y^n z + z^n x \in \mathbb{C}[x,y,z]$

$= y \cdot x^n + z^n \cdot x + y^n z \in (\mathbb{C}[y,z])[x]$

$\Rightarrow f$ irred in $\mathbb{C}(y,z)[x]$ by generalized Eisenstein criterion, $p = z \in \mathbb{C}[y,z]$

$\Rightarrow f$ irred in $(\mathbb{C}[y,z])[x] = \mathbb{C}[x,y,z]$ since primitive

$(\gcd(\text{coeffts}) = \gcd(y, z^n, y^n \cdot z) = 1.)$

(Here, the generalized Eisenstein criterion is the following: –

above $P = (p)$, principal.

Suppose $f \in R[x]$, $f = a_n x^n + \dots + a_1 x + a_0$, R UFD, $P \subset R$ prime ideal,

$a_n \notin P$, $a_0, \dots, a_{n-1} \in P$, $a_0 \notin P^2$. Then f irred in $F[x]$, $F := \text{ff } R$.

And f irred in $R[x]$ if f primitive (by Gauss Lemma).)

11. We follow the hint. Suppose f irred.

$$\underset{\substack{\| \\ a_{2n+1}x^{2n+1}+\dots+a_0}}{f = g\cdot h} = (b_m x^m + \dots + b_0)(c_\ell x^\ell + \dots + c_0) \qquad m < \ell, \quad m+\ell = 2n+1.$$

(In particular, $a_{2n+1} = b_m \cdot c_\ell \Rightarrow p \nmid b_m,\ p \nmid c_\ell$)

$\rightsquigarrow \quad a_m = b_m c_0 + b_{m-1} c_1 + \dots + b_0 c_m$

$m \le n \Rightarrow p^2 \mid a_m$ (by assumption)

Also $p \mid b_{m-1}, \dots, b_0$, $p \mid c_{\ell-1}, \dots, c_0$ using reduction mod p :-

$$\bar{f} = \bar{a}_{2n+1} \cdot x^{2n+1} = \bar{g}\cdot\bar{h} \quad \in \mathbb{Z}/p\mathbb{Z}[x]$$

$$\Rightarrow \bar{g} = \bar{b}_m \cdot x^m \ \ \& \ \ \bar{h} = \bar{c}_\ell \cdot x^\ell .$$

So $p^2 \mid b_m \cdot c_0$, $p \nmid b_m \Rightarrow p^2 \mid c_0. \Rightarrow p^3 \mid b_0 \cdot c_0 = a_0$ $\#$

$\square$.

12. $\varphi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$

$\quad f(x) \longmapsto f(\alpha)$.

a. $\ker\varphi \subset \mathbb{Q}[x]$ is a prime ideal (because $\mathbb{Q}[x]/\ker\varphi \overset{\text{FIT}}{\hookrightarrow} \mathbb{C}$

$\Rightarrow \mathbb{Q}[x]/\ker\varphi$ integral domain)

Prime ideals in $F[x]$, F field, are (0) & (f), for f irred.

(the same is true for any PID).

So $\ker\varphi = (0)$ or $\ker\varphi = (f)$, some $f \neq 0$, & replacing f w/ $\lambda \cdot f$

$\lambda \in \mathbb{Q}^\times = (\mathbb{Q}[x])^\times$, WMA f is monic.

b. $\mathbb{Q}[x]/\ker\varphi \underset{\text{FIT.}}{\xrightarrow{\sim}} \mathbb{Q}[\alpha] \subset \mathbb{C}$ $\therefore$ If α is transcendental $\mathbb{Q}[x] \xrightarrow{\sim} \mathbb{Q}[\alpha]$,

so $\mathbb{Q}[\alpha]$ is <u>not</u> a field.

If α is algebraic, $\ker\varphi = (f) < \mathbb{Q}[x]$ is maximal,

(same is true for any PID: f irred $\Leftrightarrow (f)$ maximal – since $(f) \subsetneq (g)$

$\Leftrightarrow$ $g \mid f$, f/g not a unit.)

so $\mathbb{Q}[x]/\ker\varphi \xrightarrow{\sim} \mathbb{Q}[\alpha]$ is a field. □.

13. $R/(p) = \mathbb{Z}[i]/(p) = \left(\mathbb{Z}[x]/(x^2+1)\right)/(p) = \mathbb{Z}[x]/(p, x^2+1)$

$= \left(\mathbb{Z}[x]/(p)\right)/(x^2+1) = \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$

$x^2+1 \in \mathbb{Z}/p\mathbb{Z}[x]$ irred $\Leftrightarrow$ $x^2+1 \equiv 0 \bmod p$ has no solutions

$\Leftrightarrow$ $p \equiv 3 \bmod 4$

(since $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic of order $p-1$:–

~~so $\exists\, x^2 \equiv -1 \bmod p$, $\Leftrightarrow \exists x.\ x$ has order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$~~

~~$p \neq 2$ $\Leftrightarrow$ $4 \mid p-1$.~~

$p=2$: $1^2+1 = 0 \bmod 2$.

$p \neq 2$: $\exists x.\ x^2+1 \equiv 0 \bmod p$

$\Leftrightarrow$ $\exists x.\ x \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order 4

$\Leftrightarrow$ $4 \mid p-1$, i.e. $p \equiv 1 \bmod 4$.

So, $R/(p)$ is a field $\Leftrightarrow$ $p \equiv 3 \bmod 4$.

If $p=2$ $R/(p) = \mathbb{Z}/2\mathbb{Z}[x]/(x^2+1) = \mathbb{Z}/2\mathbb{Z}[x]/(x+1)^2 \simeq \mathbb{Z}/2\mathbb{Z}[y]/(y^2)$

$x+1 \leftrightarrow y$

If $p \equiv 1 \bmod 4$

$$R/(p) = \mathbb{Z}/p\mathbb{Z}[x]\big/(x^2+1) = \mathbb{Z}/p\mathbb{Z}[x]\big/(x-\alpha)(x+\alpha)$$

$$\underset{CRT}{\simeq} \mathbb{Z}/p\mathbb{Z}[x]\big/(x-\alpha) \times \mathbb{Z}/p\mathbb{Z}[x]\big/(x+\alpha) \underset{\substack{FIT \\ \times 2}}{\xrightarrow{\sim}} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

$\square$.