$(1)^3 + (1)^2 + (1) + 1 = 4 \bmod 2 = 0$

$\Rightarrow$ 1 is a factor

$$\begin{array}{r} 1 \quad 1 \quad 1 \quad 1 \\ 1 \quad 0 \quad 1 \\ \hline 1 \quad 0 \quad 1 \quad 0 \end{array}$$

$\therefore x^3 + x^2 + x + 1 = (x-1)(x^2+1)$

but in $\mathbb{F}_2[x]$, $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$

$\Rightarrow (x-1)(x+1)(x+1)$

but $(x-1) = (x+1)$ since $-1 = 1$ in $\mathbb{F}_2[x]$

$\therefore x^3 + x^2 + x + 1 = (x+1)^3$ in $\mathbb{F}_2[x]$ ✓

b. $x^2 - 3x - 3$, $\mathbb{F}_5[x]$

$= x^2 - 3x + 2$ since $2 = -3$ in $\mathbb{F}_5[x]$

$= (x-2)(x-1)$

Both these terms are irreducible factors since they are monic monomials

$\therefore x^2 - 3x - 3 = (x-2)(x-1)$ in $\mathbb{F}_5[x]$ ✓

5

c. $x^2 + 1$, $\mathbb{F}_7[x]$

since 1, 2, 3 are the additive inverses of 4, 5, 6 respectively, only need to check if 0, 1, 2, 3 are solutions.

Since it is a monic quadratic, if it does factor, it must factor into linear terms ~~monomials~~, and thus have a solution.

$(0)^2 + 1 = 1$ $\qquad (2)^2 + 1 = 5$

$(1)^2 + 1 = 3$ $\qquad (3)^2 + 1 = 9 \bmod 7 = 2$

$\Rightarrow x^2 + 1$ has no solutions in $\mathbb{F}_7[x]$ ✓

$\therefore x^2 + 1$ is already irreducible in $\mathbb{F}_7[x]$

2. $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is ring we are working with

Since $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is a PID

but being a PID implies being a UFD

$\therefore$ $\mathbb{F}[x]$ is a UFD

Assume $\mathbb{F}[x]$ has finitely many monic irreducible polynomials, $p_1(x), \dots, p_k(x)$

(for simplicity, will refer to $p_i(x) = p_i \ \forall\ 0 \le i \le k$)

Consider $(p_1 \cdots p_k)$ and $(p_1 \cdots p_k) + 1$

by Euclid's Algorithm, $GCD(p_1 \cdots p_k, (p_1 \cdots p_k) + 1)$

$= GCD(p_1 \cdots p_k, (p_1 \cdots p_k) + 1 - (p_1 \cdots p_k))$

$= GCD(p_1 \cdots p_k, 1)$

$= 1$

5

Next, consider factoring $(p_1 \cdots p_k) + 1$ into monic irreducible polynomials,

which are prime in $\mathbb{F}[x]$

$\Rightarrow (p_1 \cdots p_k) + 1 = q_1 \cdots q_m$, where q_i $0 \le i \le m$ is a monic irreducible polynomial

Since this is a UFD, this is the only factorization

of $(p_1 \cdots p_k) + 1$ up to a unit

but then for any i, $0 \le i \le m$, $q_i \ne u p_j$ $\forall\ j$, $0 \le j \le k$ and u is a unit

if it was, then the $GCD(p_1 \cdots p_k, (p_1 \cdots p_k) + 1) = q_i \ne 1$

which is a contradiction

$\therefore$ q_i is a unique monic irreducible polynomial from

$p_1, \dots, p_k$.

Since this can be repeated for any finite list of monic irreducible

polynomials in $\mathbb{F}[x]$, the amount of such polynomials in $\mathbb{F}[x]$

cannot be finite

$\Rightarrow$ $\mathbb{F}[x]$ has infinite monic irreducible polynomials

$\square$

3. a. $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$

$\mathbb{Z}[\omega] \overset{?}{=} \mathbb{Z}[x]/(x^2+x+1)$

take two elements $a, b \in \mathbb{Z}[x]/(x^2+x+1)$ $a \neq 0, b \neq 0$

if $a \cdot b = 0$, then ab is a multiple of x^2+x+1

$\Rightarrow ab = c(x^2+x+1)$ for some $c \in \mathbb{Z}$

if a or b is a quadractic, the other is a constant

but then one must be a multiple of x^2+x+1, since x^2+x+1 is monic

if $a = (x^2+x+1)(d)$, $a = 0$ $\quad d \in \mathbb{Z}$

so $a \cdot b$ must be two monomials

but if $ab = c(x^2+x+1)$

$\Rightarrow a \mid x^2+x+1$ and $b \mid x^2+x+1$

$\Rightarrow x^2+x+1$ is factorizable

but x^2+x+1 is irreducible in $\mathbb{Z}[x]$

$\therefore ab \neq c(x^2+x+1)$ when $a \neq 0, b \neq 0$

$\Rightarrow \mathbb{Z}[x]/(x^2+x+1)$ is a domain.

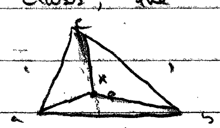
claim size function is $|z|$, where $|z|$ is the regular norm in $\mathbb{C}$

have a, b

want $a = bq + r$ where $|r| < |b|$

set $q' = a/b$, $q' \in \operatorname{Frac} \mathbb{Z}[\omega]$

since $\mathbb{Z}[\omega]$ has equilateral ~~triangle~~ lattices of length 1, as seen in class, the farthest q' is from some $q \in \mathbb{Z}[\omega]$ is $\sqrt{3}/3$ ✓



$x^2 = 1/2^2 + 1^2 = 3/4$

$\Rightarrow x = \sqrt{3}/2$

but p is $2/3$ from top vertex since triangle abp is $1/3$ the area of Δabc $\Rightarrow$ has $1/3$ the height

$\Rightarrow (\sqrt{3}/2)(2/3) = \sqrt{3}/3$ = distance from c $\Rightarrow$ distance from a and b

$\therefore |q - q'| \leq \sqrt{3}/3 < 1$ where q is nearest lattice point

$r = a - bq$

but $|q - \frac{a}{b}| = |q - q'| < |1|$

$|q - \frac{a}{b}| < |1|$ ✓

$|bq - a| < |b|$

$\Rightarrow |r| < |b|$

thus $|z|$ fits as a size function ✓

$\Rightarrow \mathbb{Z}[\omega]$ is a Euclidean Domain.

b. $\mathbb{Z}[\sqrt{-2}]$

$\mathbb{Z}[\sqrt{-2}] \cong \mathbb{Z}[x]/(x^2+2)$

take $a, b \in \mathbb{Z}[x]$, $a \neq 0$ $b \neq 0$

if $ab = 0$, then $ab = c(x^2+2)$ for some $c \in \mathbb{Z}$

if a is a constant, b is a quadratic

but x^2+2 is monic, so $b = x^2+2$ or $b = d(x^2+2)$ s.t. $ad = c$, $d \in \mathbb{Z}$

but then $b = 0 \mod x^2+2$

$\Rightarrow$ contradiction

thus a, b must be two monomials

but this implies x^2+2 factors in $\mathbb{Z}[x]$

Which it does not, since its two roots $\pm\sqrt{-2}$ are not in $\mathbb{Z}$.

$\Rightarrow$ contradiction

$\therefore ab \neq 0$ for $a \neq 0$, $b \neq 0$

$\Rightarrow \mathbb{Z}[\sqrt{-2}]$ is a domain

Claim size function is $|z|$, where $|\ |$ is the common distance function

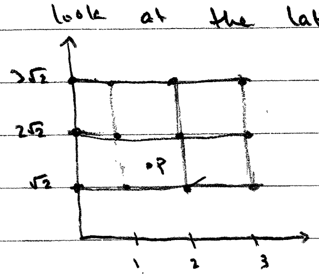
for $z \in \mathbb{Z}[\sqrt{-2}]$, $z = a + b\sqrt{2}$

$|z| = \sqrt{a^2 + 2b^2}$

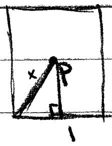
want $a = bq + r$ for some $a, b \in \mathbb{Z}[\sqrt{-2}]$

and $|b| > |r|$

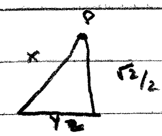
look at the lattice constructed by this ring



if $q' = \frac{a}{b} \in \operatorname{Frac} \mathbb{Z}[\sqrt{-2}]$, farthest q' can be from any point of $\mathbb{Z}[\sqrt{-2}]$ is point p



$\sqrt{2}$ $\Rightarrow$



$\Rightarrow (\sqrt{2}/2)^2 + (1/2)^2 = x^2$

$= 3/4 \quad \Rightarrow \quad x = \sqrt{3}/2$ ✓

$\therefore |q - q'| \leq \sqrt{3}/2 < 1$ where q is nearest lattice point

$r = a - bq$

$|q - q'| = |q - a/b| < |1|$

$\Rightarrow |bq - a| < |b|$ ✓

$\Rightarrow |r| < |b|$

$\Rightarrow$ the size function holds

$\Rightarrow \mathbb{Z}[\sqrt{-2}]$ is a Euclidean Domain

□

5

5

4. a. Factor $1-3i$ in $\mathbb{Z}[i]$

$(a+bi)(c+di) = 1-3i$

but if $(a+bi)$ is a factor, so is $(a-bi)$

also $(1+3i)$ is $(1-3i)(-i)$ where $-i$ is a unit in $\mathbb{Z}[i]$

$\Rightarrow$ they are factors of $(1+3i)$ as well

$\Rightarrow$ $(a+bi)(c+di) = 1-3i$
$(a-bi)(c-di) = 1+3i$) multiply by conjugates

$\Rightarrow$ $(a^2+b^2)(c^2+d^2) = 10$

but $\mathbb{Z}[i]$ is a UFD

$10 = 5 \cdot 2$ in terms of integers

$\Rightarrow$ $(a+bi)(a-bi) = 5$ and $(c+di)(c-di) = 2$ or vice versa

but 5 and 2 are factorable in $\mathbb{Z}[i]$

$(1+2i)(1-2i) = 5$ $(1-i)(1+i) = 2$

but we also proved that the primes in $\mathbb{Z}[i]$ are integer primes p s.t. $p \bmod 4 = 3$ and those ~~values~~ $\pi \in \mathbb{Z}[i]$ s.t. $\pi\bar{\pi} = p$ where $p \bmod 4 = 1$ or $p = 2$

5

$\therefore$ $(1+2i)(1-2i), (1-i), (1+i)$ are all primes, since 5 and 2 are integer primes

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

but $\Rightarrow$ $-1(1+2i)(1+i) = 1-3i$

which is okay since -1 is a unit

$\Rightarrow$ $1-3i$ factors into $(1+2i)(-1-i)$ ✓

b. Factor 10

This follows directly from part a, since we showed

$10 = 5 \cdot 2 = (1+2i)(1-2i)(1+i)(1-i)$

and also proved all those four factors are prime in $\mathbb{Z}[i]$

$\therefore$ 10 factors into $(1+2i)(1-2i)(1+i)(1-i)$ in $\mathbb{Z}[i]$ ✓

5. $\mathbb{Z}[i]/(3+4i, 4+7i)$

$GCD(3+4i, 4+7i)$ Euclid's Algorithm ✓

$= GCD(3+4i, 1+3i)$

$= GCD(2+i, 1+3i)$

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

(follows from 4 a.)

5

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

$\therefore GCD(1+3i, 2+i) = 1-2i$

$1-2i$ is definitely in the ideal, since we just used subtraction to show $2+i$ is in the ideal, and that implies $1+2i$ is in the ideal since they differ by multiplication by $-i$. ✓

Since $1-2i$ is in the ideal and it divides both $3+4i$ and $4+7i$, $1-2i$ must be a generator ✓

$\therefore (1-2i) = (3+4i, 4+7i)$

6. $R = \mathbb{Z}[\sqrt{-3}]$

assume p is a prime element of R

then $R/(p)$ is a domain

$R/(p) = \mathbb{Z}[\sqrt{-3}]/(p)$

$\cong \mathbb{Z}[x]/(x^2+3, p)$

$\cong \mathbb{Z}_p[x]/(x^2+3) = \mathbb{F}_p[x]/(x^2+3)$

$\mathbb{F}_p[x]$

domain

it follows that $\mathbb{F}_p[x]/(x^2+3)$ is a domain

$\Rightarrow (x^2+3)$ is a prime element of $\mathbb{F}_p[x]$

but $\mathbb{F}_p[x]$ is a PID, since $\mathbb{F}_p$ is a field

in a PID, irreducible and prime are equivalent

$\therefore (x^2+3)$ is irreducible in $\mathbb{F}_p[x]$ ✓

now assume (x^2+3) is irreducible in $\mathbb{F}_p[x]$

Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[x]$ is a PID

$\Rightarrow x^2+3$ is also prime, since irreducible $\Rightarrow$ prime in PID

$\therefore \mathbb{F}_p[x]/(x^2+3)$ is a domain but $\mathbb{F}_p[x]/(x^2+3) \cong \mathbb{Z}[x]/(x^2+3, p)$

$\cong \mathbb{Z}[\sqrt{-3}]/(p)$ since $\underset{x \to \sqrt{-3}}{\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}[\sqrt{-3}]}$ is surjective with kernel (x^2+3)

5

$\Rightarrow \mathbb{Z}[\sqrt{-3}]/(p)$ is a domain

$\Rightarrow p$ is prime in $\mathbb{Z}[\sqrt{-3}]$

$\therefore$ p is prime in $\mathbb{Z}[\sqrt{-3}] \Leftrightarrow (x^2+3)$ is irreducible in $\mathbb{F}_p[x]$

7. $\mathbb{Z}[i]/(p)$ p is an integer prime

case 1: $p \equiv 3 \bmod 4$

in this case, p is a prime of $\mathbb{Z}[i]$

We also proved that $\mathbb{Z}[i]$ is a Euclidean Domain in class, which is also shown in Prop 12.2.5 (c) in Artin, pg 361

but if $\mathbb{Z}[i]$ is a Euclidean Domain, it must also be a PID

in a PID, prime implies irreducible

$\therefore$ p is irreducible

but an irreducible element generates a maximal ideal in a PID, since no other ideal other than (1) contains it.

$\Rightarrow (p)$ is maximal

$\Rightarrow \mathbb{Z}[i]/p$ is a field.

case 2: $p \equiv 1 \bmod 4$

in this case, we showed in class that p is the product of two primes in $\mathbb{Z}[i]$

$\Rightarrow \pi\bar{\pi} = p$, $\pi \in \mathbb{Z}[i]$ is prime

$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(x^2+1, p)$

$\cong \mathbb{Z}_p[x]/(x^2+1) = \mathbb{F}_p[x]/(x^2+1)$

but since p is not a prime in $\mathbb{Z}[i]$, (x^2+1) in $\mathbb{F}_p[x]$ must have a root, by a theorem from class

$\Rightarrow x^2+1 = (x+\alpha)(x+\beta)$ $\alpha, \beta \in \mathbb{F}_p$

$\Rightarrow \mathbb{F}_p[x]/(x^2+1) \cong \mathbb{F}_p/((x+\alpha)(x+\beta))$

but $((x+\alpha), x+\beta)) = (1)$, since $(x+\alpha) - (x+\beta) = \alpha - \beta$ which is a unit in $\mathbb{F}_p[x]$ since $\mathbb{F}_p$ is a field

$\alpha\beta \bmod 1$

$\alpha^2 = 1$ if $\alpha = \beta$

$\Rightarrow \alpha = -1, \beta = -1$

$\Rightarrow \alpha$ and β are only the same when $p=2$

Since α must be the multiplicative inverse of β and ± 1 is a root of x^2+1 only in $\mathbb{F}_2$

$\therefore$ $x+\alpha$ and $x+\beta$ are coprime

by Chinese Remainder Theorem

5

$$\mathbb{F}_p[x]/(x^2+1) \cong \mathbb{F}_p[x]/(x+\alpha) \times \mathbb{F}_p[x]/(x+\beta)$$

$\mathbb{F}_5$

since $x+\alpha$ and $x+\beta$ are irreducible and $\mathbb{F}_p(x)$ is a PID, $\mathbb{F}_p[x]$ mod each ideal is a field. ✓

$$\therefore \mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x+\alpha) \times \mathbb{F}_p[x]/(x+\beta) \cong \mathbb{F}_p \times \mathbb{F}_p$$

which is a field cross a field. ★

case 3: $p=2$

$$\mathbb{Z}[i]/(2) \cong \mathbb{Z}[x]/(2, x^2+1)$$

$$\cong \mathbb{F}_2[x]/(x^2+1)$$

but $x^2+1 = (x-1)(x+1)$ in $\mathbb{F}_2[x]$

and $(x-1) = (x+1)$ in $\mathbb{F}_2[x]$ since $1 = -1 \bmod 2$

$$\Rightarrow (x^2+1) = (x+1)^2$$

$$\therefore \mathbb{F}_2[x]/(x^2+1) \cong \mathbb{F}_2[x]/(x+1)^2$$ ✓

$$\Rightarrow \mathbb{Z}[i]/(2) \cong \mathbb{F}_2[x]/(x+1)^2$$

These three cases cover $\mathbb{Z}[i]/(p)$ for all integer primes □

8. $x^2 - 2y^2 = 5$, $x, y \in \mathbb{Z}$

$\mathbb{Z}[\sqrt{5}]$

Since $2y^2$ is always even, x^2 must be odd

$\Rightarrow x$ must be odd

k^2

then for some k, $x = 2k+1$

$x^2 = (2k+1)^2 = 4k^2+4k+1$

$k^2+2k-4-2y^2=0$

$\Rightarrow 4k^2+4k+1 - 2y^2 = 5$

$4k^2+4k-4-2y^2=0$

$4k^2+4k-4 = 2y^2$

$2k^2+2k-2 = y^2$

$\therefore y^2$ is even, but all even squares are divisible by 4, since y^2 being even implies y being even; and since $2 \mid y$, $4 \mid y \cdot y = y^2$.

$2^2 - 2 = 2$
$3^2 - 2 = 2 \mod 5$ $\Rightarrow$ $x^2 - 2$ is irreducible in $\mathbb{F}_5[x]$

if we divide by 4, we get

$$\frac{k^2+k-1}{2} = y^2/4$$

but $k^2+k-1 = k(k+1) - 1$

$k(k+1)$ must be even $\Rightarrow$ k^2+k-1 is odd ✓

5

but then 2 does not divide it, while $4 \mid y^2$

$\Rightarrow$ we get an integer equal to a fraction that isn't an integer

$\Rightarrow$ contradiction

$\therefore$ $x^2 - 2y^2 = 5$ cannot have solutions in $\mathbb{Z}$ $\square$

9. $x^2 - 2y^2 = 7$ $\quad x, y \in \mathbb{Z}$

$x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$

$\therefore$ a factor has the form $a + b\sqrt{2}$,

where a, b are x, y respectively

logically, we then consider $\mathbb{Z}[\sqrt{2}]$ and find elements in that who, when multiplied by their conjugate, is 7.

notice that $-1, 1$ are units

as well as $\sqrt{2}+1$, $\sqrt{2}-1$

$(\sqrt{2}+1)(\sqrt{2}-1) = 2 - 1 = 1$ $\Rightarrow$ both are units

Claim that $(\sqrt{2}+1)^n$ and $(\sqrt{2}-1)^n$ are units

say $(\sqrt{2}+1)^n$ and $(\sqrt{2}-1)^n$ are units for $n \leq k$

$(3+\sqrt{2})(1+\sqrt{2})$

$(\sqrt{2}+1)^{k+1}(\sqrt{2}-1)^{k+1}$

$3 + 2 \cdot 9\sqrt{2}$

$5 + 9\sqrt{2}$

$= (\sqrt{2}+1)^k(\sqrt{2}-1)^k(\sqrt{2}+1)(\sqrt{2}-1)$

$= (1)(\sqrt{2}+1)^k(\sqrt{2}-1)^k$ which is a unit

$(3-\sqrt{2})(\sqrt{2} - [illegible])$

$\therefore$ $(\sqrt{2}+1)^{k+1}$ and $(\sqrt{2}-1)^{k+1}$ are units

$3 - 4\sqrt{2}$

$\Rightarrow$ $(\sqrt{2}+1)^n$ and $(\sqrt{2}-1)^n$ are units for all $n \in \mathbb{N}$

$3\sqrt{2} - \sqrt{2}$

$2\sqrt{2}$

consider $x = 3$ $\quad y = 1$

$-3 - 2 \quad -5 + 4\sqrt{2}$

$(3)^2 - 2(1)^2 = 9 - 2 = 7$ ✓

$\therefore$ $(3 - \sqrt{2})(3 + \sqrt{2}) = 7$

but you can multiply by units

$(1+\sqrt{2})^2$

$(\sqrt{2}+1)^2(3+\sqrt{2})(3-\sqrt{2})(\sqrt{2}-1)^2 = 7$

$3 + 2\sqrt{2}$

since $(\sqrt{2}+1)^2(\sqrt{2}-1)^2 = 1$

$= [(\sqrt{2}+1)^2(3+\sqrt{2})][(3-\sqrt{2})(\sqrt{2}-1)^2] = 7$

$= ((3+2\sqrt{2})(3+\sqrt{2}))((3-2\sqrt{2})(3-\sqrt{2}))$

$= (13+9\sqrt{2})(13-9\sqrt{2}) = 7$ ✓

$\therefore x = 13,\ y = 9$ is a solution

5

$25 - 32 = -7$

assume $(\sqrt{2}+1)^{2n}(3+\sqrt{2})(3-\sqrt{2})(\sqrt{2}-1)^{2n}$ gives a solution for $n = k$

$(\sqrt{2}+1)^{2(k+1)}(3+\sqrt{2})(3-\sqrt{2})(\sqrt{2}-1)^{2(k+1)}$

$= (\sqrt{2}+1)^2(\sqrt{2}+1)^{2k}(3+\sqrt{2})(3-\sqrt{2})(\sqrt{2}-1)^{2k}(\sqrt{2}-1)^2$

$= (\sqrt{2}+1)^2(a-b\sqrt{2})(a+b\sqrt{2})(\sqrt{2}-1)^2$

where $a = x$ $b = y$ is a solution

$= (3+2\sqrt{2})(a+b\sqrt{2})(a-b\sqrt{2})(3-2\sqrt{2})$

$= ((3a+4b)+(2a+3b)\sqrt{2})((3a+4b)-(2a+3b)\sqrt{2})$

they are conjugates ✓

$x = 3a+4b \quad y = 2a+3b$

this equation is definitely equal to 7

since we were just multiplying by units.

$(\sqrt{2}+1)^{2(k+1)}(\sqrt{2}-1)^{2(k+1)} = 1$

and $(3+\sqrt{2})(3-\sqrt{2}) = 7$

However, we have shown we can get infinitely many solutions by multiplying by $(\sqrt{2}+1)^{2n}$ and $(\sqrt{2}-1)^{2n}$ $\forall n \in \mathbb{N}$

$\Rightarrow x^2 - 2y^2 = 7$ ✓

has infinite solutions

$\square$