Solutions to assignment 6 - MA542

Chapter 18:

8) As I said in class, it need not be true that $d(1)=1$. I'll explain why, & what is actually true.

Example: If $D=F$ is a field, then the function $d: F\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$, $a \longmapsto 0$ sending every non-zero element to 0 is a size function

proof: (i) clearly $\forall a,b \in F\setminus\{0\}$, $0=d(a)\leq d(ab)=0$

(ii) $\forall a\in F$, $b\in F\setminus\{0\}$, let $q=ab^{-1}$ & $r=0$. Then $a=bq+r$ QED

So you can have a size function that is always 0 (& hence never 1)

(remark: if D is not a field, d cannot be identically zero: indeed, if $a\notin D^\times$, then for $1=aq+r$, r cannot be zero. so $d(r)<d(a)$, but there are no non-negative integers <0.)

Also, claim: if $d: D\setminus\{0\}\to\mathbb{Z}_{\geq 0}$ is a size function & $n\in\mathbb{Z}_{>0}$, define $d_n: D\setminus\{0\}\to\mathbb{Z}_{\geq 0}$, $a\longmapsto n\,d(a)$, then d_n is a size function.

proof: (i) $\forall a,b\in D\setminus\{0\}$, $d_n(a)=n\,d(a)\leq n\,d(ab)=d_n(ab)$

(ii) $\forall a\in D$, $b\in D\setminus\{0\}$ $\exists q,r$ with $a=bq+r$ with $r=0$ or $d(r)<d(b)$

Then $r=0$ or $d_n(r)=n\,d(r)<n\,d(b)=d_n(b)$

QED

So even if you had a size function with $d(a)=1$ for some a, you could redefine it so that $d(a)=n$ $\forall n\in\mathbb{Z}_{>0}$.

What is true? Let $m=$ minimum value of d. Then $u\in D\setminus\{0\}$ is a unit iff $d(u)=m$

proof: ($\Leftarrow$) If $d(u)=m$ is minimum, consider $\exists q,r$ with $1=uq+r$ with $r=0$ or $d(r)<d(u)$ since $d(u)$ is minimum $d(r)$ can't be $<d(u)$

so $r=0$ & $1=uq$ (ie. $u\in D^\times$)

($\Rightarrow$) $d(1)\leq d(1\cdot r)=d(r)$, so $d(1)=m$ is minimum

If $u\in D^\times$, $d(u)\leq d(uu^{-1})=d(1)=m$. m is minimum so $d(u)\geq m$

so $d(u)=m$ QED

14) Since $N(1-i)=1+1=2$ is prime, $1-i$ is irred.

15) $10 = 2\cdot 5$
$= (2+\sqrt{-6})(2-\sqrt{-6}) = N(2+\sqrt{-6})$

$(2+\sqrt{-6})$ is irred: if $(2+\sqrt{-6}) = ab$, $a,b \notin (\mathbb{Z}[\sqrt{-6}])^\times$, then $N(2+\sqrt{-6}) = N(a)N(b)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 10 = 2\cdot 5$

so wlog $N(a) = 2$. If $a = \alpha + \beta\sqrt{-6}$
$N(a) = \alpha^2 + 6\beta^2 = 2$. Impossible!

This also shows $(2-\sqrt{-6})$ is irred: (since $N(2-\sqrt{-6}) = 10$, too)

2 is irred: $N(2) = 4 = 2\cdot 2$ so if $2 = ab$ wlog $N(a) = 2$. Impossible from above.

So 2 is an irred. that occurs in the factorization of 10, thus if $\mathbb{Z}[\sqrt{-6}]$ were a UFD, then it must be an associate of $2+\sqrt{-6}$ or $2-\sqrt{-6}$.

The units of $\mathbb{Z}[\sqrt{-6}]$ are $\alpha + \beta\sqrt{-6}$ s.t. $N(\alpha+\beta\sqrt{-6}) = \alpha^2 + 6\beta^2 = 1$
so $(\mathbb{Z}[\sqrt{-6}])^\times = \{\pm 1\}$ $\qquad \Rightarrow \alpha = \pm 1 \quad \beta = 0$

Since $2 \neq \pm(2 \pm \sqrt{-6})$, $\mathbb{Z}[\sqrt{-6}]$ is not a UFD. QED

Every PID is a UFD, so $\mathbb{Z}[\sqrt{-6}]$ is not a PID.

18) If $7 = ab$ with $a,b \notin D^\times$ $(D = \mathbb{Z}[\sqrt{6}])$, then $49 = N(7) = N(a)N(b)$ & $N(a) = N(b) = 7$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 7\cdot 7$

write $a = \alpha + \beta\sqrt{6}$, then $N(a) = |\alpha^2 - 6\beta^2| = 7$

so $\alpha^2 - 6\beta^2 = \pm 7 \quad \alpha, \beta \in \mathbb{Z}$

look mod 7: $\alpha^2 \equiv 6\beta^2 \pmod 7$

only solutions mod 7 are $\alpha = \beta = 0$ ⟶

x	x^2	$6x^2$ mod 7
0	0	0
1	1	6
2	4	3
3	2	5
4	2	5
5	4	3
6	1	6

Thus $\alpha = 7k$, $\beta = 7l$, $k, l \in \mathbb{Z}$

so $49 \mid \alpha^2 - 6\beta^2 = \pm 7$ contradiction.

22) 2 is irred: $N(2) = 4$ so if $2 = ab$ then $N(a)N(b) = N(2) = 4 = 2\cdot 2$. If $a,b \notin D^\times$, then $N(a) = N(b) = 2$

If $a = \alpha + \beta\sqrt{5}$, then $N(a) = |\alpha^2 - \beta^2 5|$ so $\alpha^2 - \beta^2 5 = \pm 2$

look mod 5: $\alpha^2 \equiv \pm 2 \pmod 5$
$\equiv 2, 3 \pmod 5$

α	α^2 mod 5
0	0
1	1
2	4
3	4
4	1

no solutions mod 5, so no solutions in $\mathbb{Z}$

$1+\sqrt{5}$ is irred: $N(1+\sqrt{5}) = |1-5| = 4$, so as above $1+\sqrt{5}$ is irred.

$(1+\sqrt{5})(1-\sqrt{5}) = -4 = -2\cdot 2$. If $1+\sqrt{5}$ is prime then $1+\sqrt{5} \mid 2$ so $\exists\, a$ s.t. $(1+\sqrt{5})a = 2$

~~$N(1+\sqrt{5})N(a) = 4N(a) = N(2) = 4 \Rightarrow N(a) = 1 \Rightarrow a \in D^\times$~~ ↪

22) (cont'd) write $a=\alpha+\beta\sqrt{5}$, so $(1+\sqrt{5})(\alpha+\beta\sqrt{5})=2$

$$(\alpha+5\beta)+\sqrt{5}(\alpha+\beta)=2 \Rightarrow \alpha=-\beta$$

$$\alpha+5(-\alpha)=2$$

$$-4\alpha=2 \text{ impossible}$$

so $1+\sqrt{5}\nmid 2$ so $1+\sqrt{5}$ not prime

similarly, if 2 is prime, $2 \mid 1+\sqrt{5}$ so $\exists \alpha,\beta\in\mathbb{Z}$ with $2\alpha+2\beta\sqrt{5}=1+\sqrt{5}$

$\Rightarrow 2\alpha=1$ impossible

so 2 is not prime QED.

32) Let $a\in D\setminus\{0\}$, show $\exists a^{-1}\in D$. Consider decreasing chain of ideals $(a)\supseteq(a^2)\supseteq(a^3)\supseteq\cdots$

This must stabilize, ie. $\exists j>k$ s.t. $(a^j)=(a^k)$, ie. $\exists u\in D^\times$ s.t. $ua^j=a^k$.

cancel a^k on either side to get $ua^{j-k}=1$, then $a(ua^{j-k-1})=1$

so $a^{-1}=ua^{j-k-1}\in D$ QED

33) ($\Rightarrow$) Suppose R satisfies a.c.c. & let $I\trianglelefteq R$

If $\exists a_1\in I$ s.t. $I=(a_1)$ we're done.

If not $\exists a_2\in I\setminus(a_1)$. If $I=(a_1,a_2)$ we're done

keep going & get ascending chain of ideals $(a_1)\subsetneq(a_1,a_2)\subsetneq(a_1,a_2,a_3)\subsetneq\cdots$

This must end, so $\exists k$ s.t. $I=(a_1,a_2,\ldots,a_k)$ so I is finitely generated.

($\Leftarrow$) If $\exists I\trianglelefteq R$ not fin. gen'd, then $\exists a_1,a_2,\ldots\in I$ s.t.

$(a_1)\subsetneq(a_1,a_2)\subsetneq(a_1,a_2,a_3)\subsetneq\cdots$ an infinitely long strictly ascending chain

Hence R doesn't satisfy a.c.c. QED

36) solve $(1+\sqrt{2})(a+b\sqrt{2})=1$

$$(a+2b)+\sqrt{2}(a+b) \quad \text{so } a=-b \text{ & } -a=1$$

so $(1+\sqrt{2})\boxed{(-1+\sqrt{2})}=1$

for $n>0$, $(1+\sqrt{2})^n=\sum_{i=0}^{n}\binom{n}{i}\sqrt{2}^i=\sum_{j=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2j}2^j+\sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2j+1}\sqrt{2}\,2^j=\alpha_n+\sqrt{2}\beta_n$

Then $\alpha_n>1$ $\forall n>1$, so $(1+\sqrt{2})^n\neq 1$ $\forall n>0$ & ie. $\boxed{1+\sqrt{2} \text{ has infinite order}}$

Questions:

(1) Let $I\trianglelefteq D$ prime. $I=(a)$ for some $a\in D$ which is necessarily prime. Let $J\supseteq I$ proper ideal.

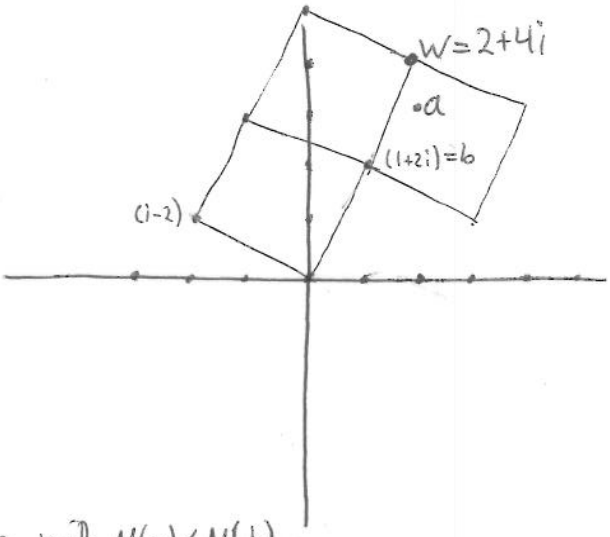
Then $\exists b\notin D^\times$ s.t. $J=(b)\supseteq(a)\Rightarrow b\mid a$. a is prime hence irred so $a=bc\Rightarrow c\in D^\times$

Then $(a)=(b)$ so I is max'l. QED

(2) $a=2+3i$, $b=1+2i$ $\quad d(\alpha+\beta i)=N(\alpha+\beta i)=\alpha^2+\beta^2$

The lattice for $b=1+2i$ in $\mathbb{Z}[i]$ is:

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



$w=2b$

$a-w=a-2b=2+3i-(2+4i)=-i$

$N(-i)=1<N(b)=5$

so $\boxed{q=2,\ r=-i}$, Then $a=bq+r$ with $N(r)<N(b)$

Other answers are possible