Please show your work. Enjoy! There are at least 150pts to earn here.

Problem 1 If I is an ideal of $\mathbb{Z}$ then $I = (n)$ for some $n \in \mathbb{Z}$. This proves $\mathbb{Z}$ is a principal ideal domain.

Let I be an ideal of $\mathbb{Z}$. Suppose $n \in I$ is the least positive element of I. Suppose $a \notin (n) = n\mathbb{Z}$ but $a \in I$. Notice, by division algorithm for $a, n \in \mathbb{Z}$ we know $\exists\, q, r \in \mathbb{Z}$ such that $a = qn + r$ for $0 \leq |r| < n$. Suppose $r \neq 0$, since I is an ideal we find $r = a - qn \in I \Rightarrow |r| \in I \Rightarrow 0 < |r| < n$ a $\rightarrow\leftarrow$ to construction of n as smallest positive element of I. If $r = 0$ then $a = qn \in (n)$ a $\rightarrow\leftarrow$ to $a \notin (n)$. In summary, $I = (n)$. //

Problem 2 Consider $\alpha = 7/13$. Is α an algebraic number? Is α an algebraic integer. Briefly explain.

Let $P(x) = 13x - 7$ observe $P(\frac{7}{13}) = 7 - 7 = 0$

thus $\alpha = 7/13$ is an <u>algebraic</u> <u>number</u>.

However, $P(x)$ is not <u>monic</u> $\Rightarrow \alpha = 7/13$ is <u>not an algebraic integer</u>

(you can prove it is not possible to attain $q(\alpha) = 0$ for $q(x) = x - c$ since $q(\alpha) = \alpha - c = 0$ $\Rightarrow c = \alpha \in \mathbb{Q}$, $c \notin \mathbb{Z}$ so $q(x)$ not allowed.

Problem 3 prove, if $1 \in I$ then $I = R$.

Suppose $1 \in I$ and I an ideal.

then for all $x \in I$ and $r \in R$, $xr \in I$.

But, $x = 1$, $r \in R$ gives $xr = r \in I$

thus $r \in R \Rightarrow r \in I \Rightarrow R \subseteq I$. Conversely $I \subseteq R$ is assumed at the outset $\therefore I = R$. //

Problem 4 Show $\mathbb{Z}[\sqrt{-14}\,] = (2, 1 + \sqrt{-14})$

<u>Goal</u>: show $1 \in (2) + (1 + \sqrt{-14})$.

$(1 + \sqrt{-14})^2 = 1 + 2\sqrt{-14} - 14 = \underbrace{-13 + 2\sqrt{-14}}_{x} \in (1 + \sqrt{-14})$

But, $\underbrace{-2\sqrt{-14}}_{y}, \underbrace{2(7)}_{z} \in (2)$. Thus, $x + y + z = 1 \in (2, 1 + \sqrt{-14})$

Thus, by Problem 3, $\underline{(2, 1 + \sqrt{-14}) = \mathbb{Z}[\sqrt{-14}]}$ //

Problem 5 find the units in $\mathbb{Z}[\sqrt{-14}\,]$

$\text{norm}(a + b\sqrt{-14}) = a^2 + 14b^2 \geq 0$

thus $\text{norm}(a + b\sqrt{-14}) = a^2 + 14b^2 = 1 \Rightarrow a = \pm 1,\ b = 0$

and so, $\boxed{z = \pm 1 \text{ only units in } \mathbb{Z}[\sqrt{-14}]}$

Problem 6 Use quadratic reciprocity to answer the following question: Can you solve $x^2 \equiv 24\,(\mathrm{mod}(31))$ for any $x \in \mathbb{Z}$?

$\left(\frac{24}{31}\right) = \left(\frac{31}{24}\right) = \left(\frac{7}{24}\right)$: by remaindering Thm for Legendre's Symbol.

24, 31 $\notin 4\mathbb{Z}+1$ hence reciprocity says $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

$= -\left(\frac{24}{7}\right)$: 24, 7 $\notin 4\mathbb{Z}+1$ so reciprocity introduces $(-)$

$= -\left(\frac{3}{7}\right)$: remaindering.

$= -\left(\frac{7}{3}\right)$: $3, 7 \notin 4\mathbb{Z}+1$

$= -\left(\frac{1}{3}\right)$: remaindering

$= -\left(\frac{(-1)(-1)}{3}\right)$: $1 = (-1)^2$

$= -\left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right)$: multiplicative prop. of $\left(\frac{p_1 p_2}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)$

$= -1\,(1)\,(1)$: $3 \notin 4\mathbb{Z}+1$.

$= -1$ thus 24 is not a square modulo 31. That is to say, $x^2 \not\equiv 24 \bmod 31$ $\forall x \in \mathbb{Z}$.//

Problem 7 Let R be a ring and I a nonzero proper ideal (proper meaning $I \neq R$). Define multiplications of cosets $I + a \in R/I$ by

$$(I + a)(I + b) = I + ab.$$

Show that this multiplication is well-defined. In particular, **show that:** if $I + a = I + a'$ and $I + b = I + b'$ then $I + ab = I + a'b'$.

$I + a = I + a' \iff a - a' \in I$

$I + b = I + b' \iff b - b' \in I$

Consider then $I + a = I + a'$ and $I + b = I + b'$. Observe

$$ab - a'b' = ab - ab' + ab' - a'b'$$
$$= a(b - b') + (a - a')b'$$

But, $b - b' \in I$ thus $a(b-b') \in I$ and $a - a' \in I \Rightarrow (a-a')b' \in I$

Hence $a(b-b') + (a-a')b' \in I$ $\therefore$ $ab - a'b' \in I$ and we deduce $I + ab = I + a'b'$.//

Problem 8 Let R be integers of $\mathbb{Q}(\sqrt{d})$ where d is squarefree. If $z = a+b\sqrt{d}$ then we define $\bar{z} = a-b\sqrt{d}$. Likewise, if A is an ideal of R then the **conjugate ideal** $\bar{A} = \{\bar{z} \mid z \in A\}$. Prove:

(a) $\overline{zw} = \bar{z} \cdot \bar{w}$ for all $z, w \in R$. (here $\cdot$ is the ring multiplication) , Let $z = a+b\sqrt{d}$, $w = x+y\sqrt{d}$

$zw = (a+b\sqrt{d})(x+y\sqrt{d}) = ax + (bx+ay)\sqrt{d} + byd$

Thus $zw = ax+byd + (bx+ay)\sqrt{d}$ hence

$\overline{zw} = ax+byd - (bx+ay)\sqrt{d}$. However,

$\bar{z}\bar{w} = (a-b\sqrt{d})(x-y\sqrt{d}) = ax+byd-(bx+ay)\sqrt{d} = \overline{zw}$.//

(b) for ideals A, B show $\overline{AB} = \bar{A} \cdot \bar{B}$ (here $\cdot$ is the multiplication of ideals)

$AB = \{ a_1b_1 + \cdots + a_kb_k \mid a_i \in A, b_i \in B\}$ by def$^{\underline{n}}$ of product.

Thus $\overline{AB} = \{ \overline{a_1b_1 + \cdots + a_nb_n} \mid a_i \in A, b_i \in B\}$.

Consider, $z \in \bar{A}\cdot\bar{B} \Rightarrow z = \bar{a}_1\bar{b}_1 + \cdots + \bar{a}_n\bar{b}_n = \overline{a_1+b_1 + \cdots + a_nb_n} \in \overline{AB}$.

Thus $\bar{A}\cdot\bar{B} \subseteq \overline{AB}$. Conversely $z \in \overline{AB} \Rightarrow \exists a_i \in A, b_i \in B$ s.t.

$z = \overline{a_1b_1 + \cdots + a_nb_n} = \bar{a}_1\bar{b}_1 + \cdots + \bar{a}_n\bar{b}_n \in \bar{A}\cdot\bar{B}$.

Thus $\overline{AB} \subseteq \bar{A}\cdot\bar{B}$ and we conclude $\overline{AB} = \bar{A}\bar{B}$.//

Problem 9 A new idea which is fun to study in a relaxed setting like a test is that of the **ideal norm**. In particular, for a nonzero ideal A we know $\bar{A}A = (k)$ for some $k \in \mathbb{Z}$ where without loss of generality we may suppose $k > 0$. Define the **ideal norm of** A by $\mathrm{N}(A) = k$.

(a) If $A = (\alpha)$ then show $\mathrm{N}(A) = \mathrm{norm}(\alpha)$.

Recall, $\mathrm{norm}(\alpha) = \alpha\bar{\alpha}$ for integers of $\mathbb{Q}(\sqrt{d})$

$A\bar{A} = (\alpha)(\bar{\alpha}) = (\alpha\bar{\alpha}) = (\mathrm{norm}(\alpha))$ $\therefore$ $N(A) = |\mathrm{norm}(\alpha)|$.

(b) If A, B are nonzero ideals then $\mathrm{N}(AB) = \mathrm{N}(A)\mathrm{N}(B)$

Recall, $\exists k, l \in \mathbb{N}$ for which $A\bar{A} = (k)$ & $B\bar{B} = (l)$.

Thus $AB\,\overline{AB} = AB\bar{A}\bar{B} = A\bar{A}\,B\bar{B} = (k)(l) = (kl)$.

$\Rightarrow N(AB) = kl = N(A)N(B)$.//

(c) If $A \mid B$ then $\mathrm{N}(A) \mid \mathrm{N}(B)$

$A \mid B$ iff $\exists C$ (an ideal) such that $B = AC$ thus

$N(B) = N(A)N(C) \Rightarrow N(A) \mid N(B)$.//

(d) an ideal whose norm is prime in $\mathbb{Z}$ is a prime ideal.

Let P be an ideal and $N(P) = p$ a prime in $\mathbb{N}$.

Suppose $P \supseteq AB \Rightarrow P \mid AB \Rightarrow AB = PC$ for some ideal C.

Hence $N(A)N(B) = N(P)N(C) \Rightarrow N(P) \mid N(A)N(B)$

$\Rightarrow p \mid N(A)N(B) \Rightarrow p \mid N(A)$ or $p \mid N(B)$

Problem 10 Prove $(3 - \sqrt{-14})$ is prime in $\mathbb{Z}[\sqrt{-14}\,]$. Hint: ~~17 is prime.~~ BAD "HINT"

$N(3 - \sqrt{-14}) = \text{norm}\,(3 - \sqrt{-14}) = 9 + 14 = 23 \leftarrow$ prime.

Thus $(3 - \sqrt{-14})$ is prime ideal of $\mathbb{Z}[\sqrt{-14}]$

Problem 11 Show that $(3 - \sqrt{-14})$ is maximal in $\mathbb{Z}[\sqrt{-14}\,]$.

Prime $\Rightarrow$ Maximal in $\mathbb{Z}[\sqrt{-14}]$ $\therefore$ $(3 - \sqrt{-14})$ is maximal.

Alternatively, could show $(3 - \sqrt{-14})$ is maximal by some direct arguments. (no one attempted that route)

Problem 12 Mordell's Equation: to find integer solutions of $y^2 + 26 = x^3$ we can guess the simple solutions $x = 3$ and $y = \pm 1$. However, less trivial solutions may be found from factoring in $\mathbb{Z}[\sqrt{-26}]$. Conjecture:

$$x^3 = y^2 + 26 = (y - \sqrt{-26})(y + \sqrt{-26}) \;\;\Rightarrow\;\; y + \sqrt{-26} = (a + b\sqrt{-26})^3$$

for some $a, b \in \mathbb{Z}$. Derive two integer solutions from the above conjecture.

$$\begin{aligned} y + \sqrt{-26} = (a + b\sqrt{-26})^3 &= a^3 + 3a^2b\sqrt{-26} + 3a(b\sqrt{-26})^2 + (b\sqrt{-26})^3 \\ &= a^3 + 3a^2b\sqrt{-26} - 78ab^2 - 26b^3\sqrt{-26} \\ &= \underbrace{(a^3 - 78ab^2)}_{y} + \underbrace{(3a^2b - 26b^3)}_{1 = (3a^2 - 26b^2)b \;\to\; b = \pm 1}\sqrt{-26} \end{aligned}$$

Thus, $b = 1 \Rightarrow 1 = 3a^2 - 26 \Rightarrow 3a^2 = 27 \Rightarrow \underline{a = \pm 3}$.
$b = -1 \Rightarrow 1 = 26 - 3a^2 \Rightarrow 3a^2 = 25 \Rightarrow a \notin \mathbb{Z}$.

We find $a = \pm 3,\ b = 1 \Rightarrow y = (\pm 3)^3 \mp (78)(3)$

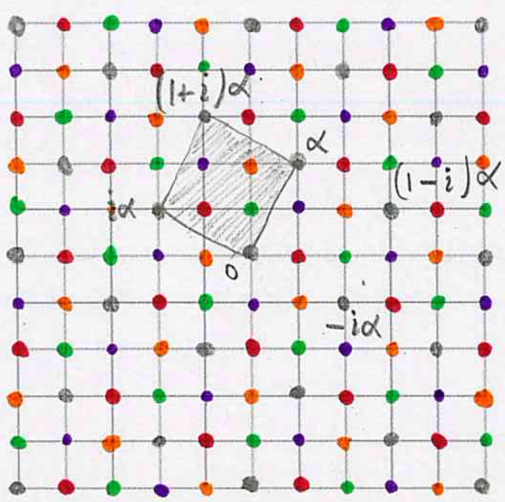
$\Rightarrow y = 27 - 3(78)$ or $-27 + 3(78)$

$\Rightarrow y = \pm 207$

But, $x = ((207)^2 + 26)^{1/3} = 35$ $\therefore$ $\boxed{(35, \pm 207) \text{ are sol}^{\text{n}}\text{'s}}$

Problem 13 Let $R = \mathbb{Z}[i]$ and consider $J = (1+2i)$. Show J is a lattice by finding $\alpha, \beta \in R$ for which $J = \{m\alpha + n\beta \mid m, n \in \mathbb{Z}\}$. Picture the ideal J and, with the help of your picture, describe the structure of R/J. In particular, find a representative for each distinctl coset in R/J. (there are 5).

$$\left.\begin{aligned} \alpha &= 1+2i \\ i\alpha &= i-2 \end{aligned}\right\} \text{ integral basis for lattice } J$$



pick any fundamental region, I prefer the one near 0 which I shaded

I represented by •

• is $I + 2i$

• is $I + 2i - 1$

• is $I + i$

• is $I + i - 1 = I + 1 = 1_{R/J}$

• is $I + 0 = I = 0_{R/J}$

Let $I = \bar{0}$, $I + i - 1 = \bar{1}$, $I + i = \bar{i}$, $I + 2i - 1 = \overline{2i-1}$, $I + 2i = \overline{2i}$

Challenge: are there zero divisors in R/J ? If not, can you find a finite field which is ring isomorphic to R/J ?

$\times$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{2i-1}$	$\overline{2i}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{2i-1}$	$\overline{2i}$
$\bar{i}$	$\bar{0}$	$\bar{i}$	$\overline{2i}$	$\bar{1}$	$\overline{2i-1}$
$\overline{2i-1}$	$\bar{0}$	$\overline{2i-1}$	$\bar{1}$	$\overline{2i}$	$\bar{i}$
$\overline{2i}$	$\bar{0}$	$\overline{2i}$	$\overline{2i-1}$	$\bar{i}$	$\bar{1}$

$\bar{i}\,\bar{i} = \overline{-1} = \overline{2i}$

$\bar{i}(\overline{2i-1}) = \overline{-2-i} = \bar{1}$

$\bar{i}(\overline{2i}) = \overline{-2} = \overline{2i-1}$

$\overline{2i-1}^{\,2} = \overline{-2}^{\,2} = \bar{4} = \overline{2i}$

$\overline{2i}(\overline{2i-1}) = \overline{-4i} = \bar{i}$

$\overline{2i}\;\overline{2i} = \overline{-4} = \bar{1}$

$\bar{4}\bar{4} = \overline{16} = \bar{1} \longrightarrow \overline{2i} \longleftrightarrow \bar{4}$

$\bar{2}\bar{2} = \bar{4} \longrightarrow \bar{i} \longleftrightarrow \bar{2}$

Compare to $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

You can prove, $R/J \approx \mathbb{Z}_5$.

Problem 14 Recall the equivalence of the following properties of an ideal P:

$$(1.)\ AB \subseteq P \ \Rightarrow\ A \subseteq P \text{ or } B \subseteq P, \qquad\qquad (2.)\ ab \in P \ \Rightarrow\ a \in P \text{ or } b \in P$$

Please prove just one direction of (1.) $\Leftrightarrow$ (2.). (your choice)

– See pg. 212 in Stillwell. –

Problem 15 Prove: every maximal ideal is prime.

– See page 213 in Stillwell –

Problem 16 Explain why every prime ideal is maximal in the integers of an imaginary quadratic field.

– page 226 in Stillwell, but perhaps the proof I shared in class was more complete. Once I update LECTURE 24 it should be at the end.