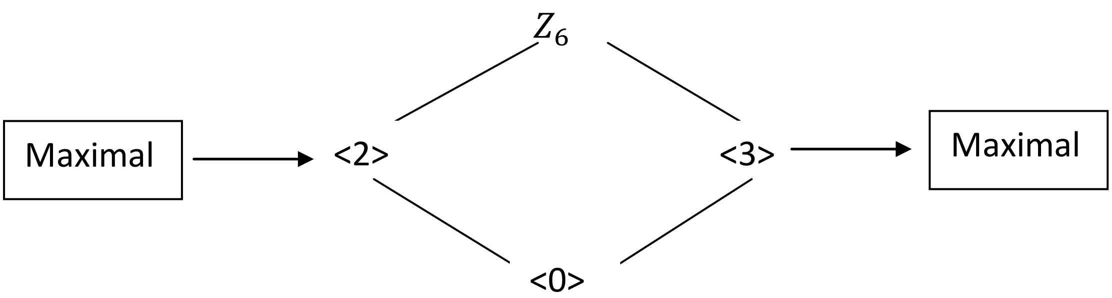
Homework (1)

1) Find all prime and maximal ideals in Z_6 and $Z_2 \times Z_4$.

Z_6 = {0, 1, 2, 3, 4, 5} is a commutative ring with unity.

$\odot$ mod 6	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

<0> = {0} is neither prime nor maximal ideal (Z_6 is not integral domain)
<1> = <5> = Z_6 (generators). Again neither prime nor maximal.
<2> = <4> = {0, 2, 4} $\Rightarrow$ Prime ideal.
<3> = {0, 3} $\Rightarrow$ Prime ideal.
To find out the maximal:



Remember: In a commutative ring with 1, every maximal ideal is prime. (The converse is not true. For example: <0> is prime in integral domains, but clearly not maximal).

$Z_2 \times Z_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$ is commutative ring with unity. (Not integral domain: (0, 2) (0, 2) = (0, 0))
$<(0,0)>$ is neither prime nor maximal ideal
$<(1,1)> = <(1,3)> = Z_2 \times Z_4$ again neither prime nor maximal ideal
$<(0,1)> = \{(0,0), (0,1), (0,2), (0,3)\} = <(0,3)>$ (Maximal)
$<(1,2)> = \{(0,0), (0,2), (1,0), (1,2)\}$ (Maximal)
$<(0,2)> = \{(0,0), (0,2)\}$ (Not maximal since < (0, 2)> $\subset$ < (0, 1)>)
$<(1,0)> = \{(0,0), (1,0)\}$ (Not maximal since < (1, 0)> $\subset$ < (1, 2)>)

Or:

By Theorem: *Let R be a commutative ring with $1 \in R$; and M be an ideal of R. Then M Is maximal (prime) ideal $\Leftrightarrow$ R/M is a field (integral domain)*

So we must find all M for which $Z_2 \times Z_4/M$ is an integral domain. But if M is proper and nontrivial, then $Z_2 \times Z_4/M$ as an Abelian group, is isomorphic to one of the following: Z_2, Z_4, $Z_2 \times Z_2$. The only integral domain is Z_2. So $|M|$ should be "4" which makes M isomorphic to either $Z_2 \times Z_2$ or Z_4.This M will be both prime and maximal ideal. So, $\boldsymbol{M = <(0,1)>}$ or $M =<(\mathbf{1},\mathbf{2})>$.

2) Find all $c \in Z_3$ such that $Z_3/<x^2+1>$ is a field.

Using the following theorems:

(i) Let F be a field and let I be an ideal of the polynomial ring $F[x]$. Then

1. I is maximal if and only if $I =<p(x)>$ for some irreducible polynomial $p(x)$ in $F[x]$.

2. I is prime if and only if $I = \{0\}$ or $I =<p(x)>$for an irreducible $p(x) \in F[x]$.

(ii) Let R be a commutative ring with $1 \in R$; and M be an ideal of R. Then
M is maximal ideal $\Leftrightarrow$ R/M is a field

∴ $Z_3[X]/<x^2 + c>$ is a field $\Leftrightarrow$ $<x^2 + c>$ is maximal ideal.
$<x^2 + c>$ is maximal ideal iff x^2+c is irreducible.
The possibilities are:
$p(x) = x^2$ then, $p(0) = 0 \implies$ p(x) is reducible $\implies$ $<x^2>$ is not maximal.

$p(x) = x^2 + 1$ then, $p(0) = 1$, $p(1) = 2$, and $p(2) = 2 \implies$ p(x) is irreducible
$\implies$ $<x^2 + 1>$ is a maximal ideal $\implies$ $Z_3[X]/<x^2 + 1>$ is a field

$p(x) = x^2 + 1$ then, $p(1) = 0 \implies$ p(x) is reducible $\implies$ $<x^2+2>$ is not maximal.

Therefore, c = 1.

3) Show that N is a maximal ideal in a ring R $\Leftrightarrow$ R/N is a simple ring.

Let R be a commutative ring with $1 \in R$.
If N is a maximal ideal in R, then by theorem, R/N is a field.
$\implies$ R/N is also a commutative ring with unity (1+N)
So by theorem 1.3.16, R/N is a field $\Leftrightarrow$ R/N is simple.
Therefore, N is a maximal ideal in R $\Leftrightarrow$ R/N is a simple ring.

4) Let A and B be ideals of a commutative ring . the quotient $A : B$ of A by B is defined by $A{:}B = \{r \in R : rb \in A \ \forall\, b \in B\}$. Show that $A : B$ is an ideal of R.

Let $r_1, r_2 \in A{:}B$ $\implies r_1 b \in A \quad \forall\, b \in B$
$\implies r_2 b \in A \quad \forall\, b \in B$

i. $r_1 - r_2 \in A{:}B$?
(We have to show $(r_1 - r_2)b \in A \quad \forall\, b \in B$)
Let $b \in B$, consider,

$(r_1 - r_2)b = r_1 b - r_2 b \in A$ (since $r_1 b \in A$ and $r_2 b \in A$ and A is an ideal)
Since b is arbitrary
$\therefore (r_1 - r_2)b \in A \quad \forall\, b \in B \implies r_1 - r_2 \in A{:}B$

ii. Let $s \in R$. $sr_1 = r_1 s \in A{:}B$?
Consider,
$(r_1 s)b = (sr_1)b = s(r_1 b) \in A$ (since A is an ideal and $r_1 b \in A$)
$\therefore (sr_1)b = (r_1 s)b \in A \quad \forall\, b \in B \implies sr_1, r_1 s \in A{:}B$

5) Find all zero divisors; and nonzero idempotent, units and nilpotent elements in $Z_3 \oplus Z_6$.

$Z_3 \oplus Z_6 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5), (2,0), (2,1), (2,2), (2,3), (2,4), (2,5)\}$

(i) Zero Divisors:
(we have to find: $(r_1,s_1) \neq (0,0)$ and $(r_2, s_2) \neq (0,0)$ s.t. $(r_1, s_1)(r_2, s_2) = (0, 0)$)

Since: (0, 2) (0, 3) = (0, 0)
(0, 3) (0, 4) = (0, 0)

∴ The zero divisors are: (0, 2), (0, 3) and (0, 4)

(ii) Idempotent Elements: ($a \neq 0$ s.t. $a^2 = a$?)

Since: (0, 1) (0, 1) = (0, 1)
(0, 3) (0, 3) = (0, 3)
(0, 4) (0, 4) = (0, 4)
(1, 0) (1, 0) = (1, 0)
(1, 1) (1, 1) = (1, 1)
(1, 3) (1, 3) = (1, 3)
(1, 4) (1, 4) = (1, 4)

∴ The idempotent elements are: (0,1), (0,3), (0,4), (1,0), (1,1), (1,3) and (1,4).

(iii) Nilpotent Elements: ($a^n = 0$ for some $n \geq 1$?)

Since Z_3 is an integral domain then it has no nilpotent element.
Then, $(r, s)^n = (0, s^n) = (0, 0)$. We have to find the nilpotent elements in Z_6.
Since the nilpotent elements should be different from the idempotent ones, so we can eliminate 1, 3 and 4 away. (**Since** $\mathbf{3^n = 3}$ **and** $\mathbf{4^n = 4}$ $\forall\, \boldsymbol{n} > 1$)
To find the nilpotent elements we should solve the equation $x^2 = 0$ **(by Theorem: *R* has no nonzero nilpotent elements if and only if 0 is the unique solution of the equation $\boldsymbol{x^2 = 0}$)**

If $x = 2 \implies x^2 = 2^2 = 4 \neq 0$
If $x = 5 \implies x^2 = 5^2 = 1 \neq 0$ (unit)
$\therefore 0$ *is the unique solution of* $\boldsymbol{x^2 = 0}$
$\therefore Z_6$ has no nilpotent elements , so that $Z_3 \oplus Z_6$

(iv) Units: $((r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (1, 1)?$)

So the units are: (1,1), (1,5), (2,1),and (2,5).

6) Suppose that a and b belong to a commutative ring, and ab is a zero divisor. Show that either a or b is a zero divisor.

Let $a, b \in R$ where R is a commutative ring and ab is a zero divisor such that b is not a zero divisor. (We have to show that a is a zero divisor).

$\Longrightarrow \exists\, 0 \neq x \in R$ s.t. $x(ab) = 0$

$\Longrightarrow$ $(xa)b = 0$ (So that $(xa) = 0$)

$\Longrightarrow$ $xa = 0$ (Since b is not a zero divisor)

$\therefore\ \exists\, 0 \neq x \in R$ s.t. $xa = 0 = ax \Longrightarrow a \text{ is a zero divisor}.$

Similarly if a is not a zero divisor, then b will be.

7) Prove that $I = < 2 + 2i >$ is not a prime ideal of $Z[i]$. What is the characteristic of $Z[i]/I$?

$Z[i] = \{a + bi :\ a, b \in \mathbb{Z}\}$ is a commutative ring with 1 .

Then $I =< 2 + 2i >$ is prime if $I \neq Z[i]$ and if

$$ab \in I \Longrightarrow a \in I \text{ or } b \in I \quad \forall a, b \in Z[i]$$

$I = \{z(2 + 2i): z \in Z[i]\} = \{(a + bi)(2 + 2i): a, b \in \mathbb{Z}\}$

$= \{2(a - b) + 2(a + b)i: a, b \in \mathbb{Z}\}$

But we have:

(1+3 i)(3+3 i) = (3-9) + (3+9) i = -6 + 12 i $\in I$ where (1+3 i), (3+3 i) $\notin I$

$$\therefore\ \exists\, xy \in I \quad s.t. \quad x \notin I \ \text{ and }\ y \notin I \Longrightarrow I \text{ is not prime}.$$

$Z[i]/I = \{(a + bi) + I : a, b \in \mathbb{Z}\} = \{I,\ 1 + I,\ 2 + I,\ 3 + I, (1 + i) + I,\ i + I, \dots\}.$

The characteristic of $Z[i]/I$ is "4".

- How to deal with the Gaussian Integers? Page 5

8) Show that $Z_3[X]/ < x^2 + x + 1 >$ is not a field.

Since (x+2) $\in Z_3[X] \Rightarrow$ (x+2) + $I \in Z_3[X]/ I$ where I=<x^2+x+1>

But,

((x+2) +I) ((x+2) +I) = (x^2+x+1) + I = < x^2+x+1 > =I

$\therefore$ (x+2) + I is a zero divisor $\Longrightarrow$ $Z_3[X]/ I$ is not a field.

9) Prove that M is a maximal ideal in a commutative ring R with unity iff $\forall\, x \notin M\ \exists\, r \in R$ such that $1 + rx \in M$.

" $\Longrightarrow$ "

Let M be a maximal ideal in a commutative ring R with unity.

Let $x \notin M$.

Construct $I = \{m + xr: \quad m \in M, \quad x \notin M\}$. Then I is an ideal of R.

(Let $z, y \in I, \quad \grave{r} \in R \Longrightarrow \quad y = m_1 + xr_1$ and $z = m_2 + xr_2$

i. $y - z = m_1 + xr_1 - (m_2 + xr_2) = (m_1 - m_2) + x(r_1 - r_2) \in I$

Since $m_1 - m_2 \in M$ (M is an ideal)

ii. $y\grave{r} = \grave{r}y = \grave{r}(m_1 + xr_1) = \grave{r}m_1 + \grave{r}(xr_1) = \grave{r}m_1 + x(\grave{r}r_1) \in I$

Since $\grave{r}m_1 \in M$ (M is an ideal) and $\grave{r}r_1 \in R$))

Therefore, I is an ideal of R such that $M \subset I \subseteq R$.

i. $m \in M \Rightarrow m = m + x.0 \in I$

ii. $x \notin M$ and $x = 0 + x.1 \in I$ (So that $M \neq I$)

But M is maximal $\Longrightarrow I = R \Longrightarrow 1 \in I \Longrightarrow 1 = m + xr \Longrightarrow m = 1 - rx$

$\Longrightarrow m = 1 + \grave{r}x \in M$

$\therefore\ \forall\, x \notin M\ \exists\, \grave{r} \in R$ such that $1 + \grave{r}x \in M$.

" $\Longleftarrow$ "

Assume that $\forall\, x \notin M \quad \exists\, r \in R$ such that $1 + rx \in M$.

(We have to prove that M is a maximal ideal)

Let I be an ideal of R such that $M \subset I \subseteq R$. (We have to prove $I = R$).

The proper inclusion implies that $\exists\ x \in I$ where $x \notin M$.

By given; $\exists\, r \in R$ such that $1 + rx \in M \subset I \Longrightarrow m = 1 + rx \in I$.

$\Longrightarrow 1 = m - rx \in I \quad \Longrightarrow \quad I = R \quad \Longrightarrow M$ is a maximal ideal of R.

Since $x \in I$ and I is an ideal $\Longrightarrow rx \in I$ also $m \in I \Longrightarrow m - rx \in I$ (ideal)

Finding Factor Rings over the
Gaussian Integers

He [Gauss] lives everywhere in mathematics. (E.T. Bell, "Men of Mathematics").

Some Important theorems that may help:

- $Z[i\,]$ is a PID. (i.e. every ideal is principal)
- The characteristic of $Z[i\,]/< a + bi >$ divides $a^2 + b^2$.
- $Z[i]/< a + bi > \cong Z[i]/< -a - bi > \cong Z[i]/< b - ai > \cong Z[i]/< -b + ai >$
- If " a " is a positive integer larger than 1, then

$$Z[i]/< a > \cong Z_a[i]$$

- If a and b are relatively prime integers, then $Z[i\,]/< a + bi > \cong Z_{a^2+b^2}$
- The primes in $Z[i\,]$ are:
  - i. $a + bi$ and $b + ai$ where $p = a^2 + b^2$ is prime in $\mathbb{Z}$ and $p \equiv 1 \ (mod\ 4)$
  - ii. p where p is prime in $\mathbb{Z}$ and $p \equiv 3 \ (mod\ 4)$
  - iii. $1 + i$
- If a and b are relatively prime integers, then
  $a + bi$ is a prime in $Z[i\,]$ $\Leftrightarrow$ $a^2 + b^2$ is prime in $\mathbb{Z}$.

- So we can conclude that : $Z[i\,]/\,I$ is an integral domain $\Leftrightarrow$ I is a prime ideal $\Leftrightarrow$
  - i. $I =< a >$ where a is prime in $\mathbb{Z}$ and $a \equiv 3 \ (mod\ 4)$.
  - ii. $I =< a + bi >$ where a and b are relatively prime integers and $a^2 + b^2$ is prime in $\mathbb{Z}$.

Back to problem "7", we notice the following:

$(2 + 2i) = (2(1 + i))$ is not prime in $Z[i]$ $\Longrightarrow$ $I =< 2 + 2i >$ is not a prime ideal in $Z[i]$. ($a = 2 = b$ not relatively prime and $a^2 + b^2$ =8 (not prime in $\mathbb{Z}$)).

Also we can prove that I is not prime by finding x and y such $xy \in I$ but $x \notin I$ *and* $y \notin I$

$$I =< 2 + 2i >= \{2(a - b) + 2(a + b)i: \qquad a, b \in \mathbb{Z}\}$$

$\mathbf{2(1 + i) = 2 + 2i \in I}$ **But, $2 \notin I$**

(Since, we want to find $a, b \in \mathbb{Z}$ s.t $2(a - b) = 2 \quad (\mathbf{1})$ and
$2(a + b) = 0 \quad (\mathbf{2})$

$\Rightarrow a - b = 1 \quad \Rightarrow \quad a = 1 + b$ **(From (1)**)

$\Rightarrow a + b = 0 \quad \Rightarrow \quad 1 + 2b = 0 \quad \Rightarrow b = -\frac{1}{2} \notin \mathbb{Z} \quad \Rightarrow 2 \notin I$)

Also, $\mathbf{1 + i \notin I}$.

(Since, we want to find $a, b \in \mathbb{Z}$ s.t $2(a-b) = 1$ $(\mathbf{1})$ and
$2(a+b) = 1$ $(\mathbf{2})$

$\Longrightarrow a - b = \frac{1}{2}$ $\Longrightarrow$ $a = \frac{1}{2} + b$ **(From (1)**) $\Longrightarrow$ clearly $a \notin \mathbb{Z}$ $\Longrightarrow 1 + i \notin I$)

$$\Longrightarrow \quad Z[i]/I = \{(c + di) + I: \quad c, d \in \mathbb{Z}\}$$

$$= \{2(a-b) + c + (2(a+b) + d)i: \quad a, b, c, d \in \mathbb{Z}\}$$

- Greg Dresden and Wayne M. Dyma`cek, "Finding Factors of Factor Rings over the Gaussian Integers", THE MATHEMATICAL ASSOCIATION OF AMERICA (2005): 602-611
- PETER J. KAHN, "TRISECTION, PYTHAGOREAN ANGLES, AND GAUSSIAN INTEGERS", (2011).
- Rachel Quinlan, his lectures notes as published in http://www.maths.nuigalway.ie/MA416/#Lecturer.

Written by: Fatma Sharaf (2011)