Sam Lloyd: 994948

MAST20022, Group Theory and Linear Algebra, Assignment 1

Q1:

① $a|b$, i.e. $a = qb$ for some $q \in \mathbb{Z}$

② $\gcd(a,b) = a$, i.e. $a|a \wedge a|b$,

$\langle c|a \wedge c|b \rangle \Rightarrow c|a$, for $\forall c \in \mathbb{Z}$

① ⇒ ②

proof:

$a|b$, let $q=1$ in the definition

$a|a$, trivially $a = 1 \times a$

$\therefore a|b \wedge a|a$

let $c \in \mathbb{Z}$ such that $c|a \wedge c|b$

$\Rightarrow c|a$

$\therefore \langle c|a \wedge c|b \rangle \Rightarrow c|a$ □

② ⇒ ①

proof:

$\gcd(a,b) = a \Rightarrow a|a \wedge a|b$

$\Rightarrow a|b$ □

Therefore ① ⇔ ②

i.e. $a|b \iff \gcd(a,b) = a$

Q2:

a) $\gcd(12378, -3054)$

$= \gcd(12378, 3052)$, Lemma 1.8:1)

$12378 = 4 \times 3054 + 162$

$3054 = 18 \times 162 + 138$

$162 = 1 \times 138 + 24$

$138 = 5 \times 24 + 18$

$24 = 1 \times 18 + 6$

$18 = 3 \times 6 + 0$

ie. $\gcd(18, 24) = 6$

therefore $\gcd(12378, -3054) = 6$

b)

$$
\begin{aligned}
6 &= (24) - 1\times(18) \\
&= (162 - 1\times138) - 1\times(138 - 5\times24) \\
&= (162 - 1\times138) - 1\times(138 - 5\times(162 - 1\times138)) \\
&= 6\times(162) - 7\times(138) \\
&= 6\times(162) - 7\times(3054 - 18\times162) \\
&= 132\times(162) - 7\times(3054) \\
&= 132\times(12378 - 4\times3054) - 7\times(3054)
\end{aligned}
$$

$\therefore 6 = 132\times(12378) - 535\times(3054) = 132\times(12378) + 535(-3054)$

therefore $x = 132$, $y = 535$

Q3:

a) i)

$$\begin{cases} [2]_5 x + [3]_5 y = [4]_5 & \text{— } ① \\ [3]_5 x + [-2]_5 y = [1]_5 & \text{— } ② \end{cases}$$

① ← ①+② $\Rightarrow [5]_5 x + [1]_5 y = [5]_5$

$\Rightarrow \cancel{[1]_5 y}\ [0]_5 x + [1]_5 y = [0]_5$

$\Rightarrow [y]_5 = [0]_5$ —— ③

③ → ② $\Rightarrow [3]_5 x + [-2]_5 [0]_5 = [1]_5$

$\Rightarrow [3]_5 x = [1]_5$

$\Rightarrow [2]_5 [3]_5 x = [2]_5 [1]_5$

$\Rightarrow [1]_5 x = [2]_5$

$\Rightarrow [x]_5 = [2]_5$

Therefore $x = [2]_5$, $y = [0]_5$

NB: Scalar multiplication is not defined for congruence classes, we should have $[5]_5 [x]_5$ etc

~~b)~~ ii)

$$\begin{cases} [2]_{11} x + [3]_{11} y = [4]_{11} & \text{— } ① \\ [3]_{11} x + [-2]_{11} y = [1]_{11} & \text{— } ② \end{cases}$$

① ← ① × $[7]_{11}$ $\Rightarrow$ $[3]_{11} x + [-1]_{11} y = [6]_{11}$

② ← ② − 2 × ① $\Rightarrow$ $[-3]_{11} x + [0]_{11} y = [-11]_{11}$

$\Rightarrow [-3]_{11} x = [0]_{11} + [0]_{11} y$

$\Rightarrow [-4]_{11} [-3]_{11} x = [0]_{11}$

$\Rightarrow [1]_x = [0]_{11}$

$\Rightarrow [x]_{11} = [0]_{11}$

$\therefore x = [0]_{11}$ —— ③

③ → ① $\Rightarrow [2]_{11} \cdot [0]_{11} + [3]_{11} y = [4]_{11}$

$\Rightarrow [4]_{11} [3]_{11} y = [4]_{11} [4 - 2 \cdot 0]_{11}$

$\Rightarrow [1]_{11} y = [5]_{11}$

$\Rightarrow [y]_{11} = [5]_{11}$

$\therefore y = [5]_{11}$

therefore $x = [0]_{11}$, $y = [5]_{11}$

Q3:

b) trial and error:

x	$x^3 + 3x^2 + 2x$
$[0]_{10}$	$[0]_{10}$
$[1]_{10}$	$[6]_{10}$
$[2]_{10}$	$[4]_{10}$
$[3]_{10}$	$[0]_{10}$
$[4]_{10}$	$[0]_{10}$
$[5]_{10}$	$[0]_{10}$
$[6]_{10}$	$[6]_{10}$
$[7]_{10}$	$[4]_{10}$
$[8]_{10}$	$[0]_{10}$
$[9]_{10}$	$[0]_{10}$

therefore $x = [0]_{10}, [3]_{10}, [4]_{10}, [5]_{10}, [8]_{10}, [9]_{10}$

Q4:

First, we show that $\mathbb{Q}(i)$ is a commutative ring

~~① $\forall x,y,z \in \mathbb{Q}(i)$~~ let

let $x+yi$, $a+bi$, $\alpha+\beta i$ be elements of $\mathbb{Q}(i)$

ie. $x, y, a, b, \alpha, \beta \in \mathbb{Q}$

and 0 represent $0+0i$, 1 represent $1+0i$

① $[(x+yi)+(a+bi)]+(\alpha+\beta i)$

$= [(x+a)+(y+b)i]+(\alpha+\beta i)$

$= (x+a+\alpha)+(y+b+\beta)i$

Similarly

$(x+yi)+[(a+bi)+(\alpha+\beta i)]$

$= (x+a+\alpha)+(y+b+\beta)i$ □

$\therefore$ associative addition

② $(x+yi)+(a+bi)$

$= (x+a)+(y+b)i$

$= (a+bi)+(x+yi)$

$\therefore$ commutative addition

③ 0 satisfies

$(a+bi)+0 = (a+bi)$ $\therefore$ additive identity

④ for $a+bi$, $-a-bi$ satisfies

$(a+bi)+(-a-bi) = 0$ $\therefore$ additive inverse

⑤ $[(a+bi)\times(\alpha+\beta i)]\times(x+yi)$

$= [(a\alpha - b\beta)+(a\beta+b\alpha)i]\times(x+yi)$

$= (xa\alpha - xb\beta)+(xa\beta+xb\alpha)i + (ya\alpha - yb\beta)i - (ya\beta+yb\alpha)$

$= (xa\alpha - xb\beta - ya\beta - yb\alpha) + (xa\beta + xb\alpha + ya\alpha - yb\beta)i$

$(a+bi)\times[(\alpha+\beta i)\times(x+yi)]$

$= (a+bi)\times[(\alpha x-\beta y)+(\alpha y+\beta x)i]$

$= a(\alpha x-\beta y)+a(\alpha y+\beta x)i + bi(\alpha x-\beta y) - b(\alpha y+\beta x)$

$= (xa\alpha - y\beta a - b\alpha y - b\beta x) + (a\alpha y + a\beta x + \alpha bx - \beta by)i$

$= (xa\alpha - xb\beta - ya\beta - yb\alpha) + (xa\beta + xb\alpha + ya\alpha - yb\beta)i$

$\therefore$ ~~multip~~ Associative multiplication

(6) $(a+bi)(x+yi)$

$= a(x+yi) + bi(x+yi)$

$= ax + ayi + bxi - by$

$= (ax-by) + (ay+bx)i$

$(x+yi)(a+bi)$

$= x(a+bi) + yi(a+bi)$

$= ax + bxi + ayi - by$

$= (ax-by) + (ay+bx)i$

$\therefore$ commutative multiplication

(7) for any $a+bi$, 1 satisfies

$1 \times (a+bi) = a+bi$

$\therefore$ multiplicative identity

(8) $(x+yi)[(a+bi)+(\alpha+\beta i)]$

$= x[(a+\alpha)+(b+\beta)i] + yi[(a+\alpha)+(b+\beta)i]$

$= ax + \alpha x + bxi + \beta xi + yai + y\alpha i - yb - y\beta$

$= (ax+\alpha x - by - \beta y) + (bx + \beta x + ay + \alpha y)i$

$(x+yi)(a+bi) + (x+yi)(\cancel{a+bi}\ \alpha+\beta i)$

$= ax - by + bxi + ayi + \alpha x - \beta y + \beta xi + \alpha yi$

$= (ax + \alpha x - by - \beta y) + (bx + \beta x + ay + \alpha y)i$

$\therefore$ distributative

Therefore, $\mathbb{Q}(i)$ is a commutative ring

$0, 1 \in \mathbb{Q}(i)$ and for any $a+bi$

$\frac{a-bi}{a^2+b^2} \in \mathbb{Q}(i)$ satisfies the multiplicative inverse property

$$\frac{a-bi}{a^2+b^2} \times a+bi = \frac{(a-bi)(a+bi)}{a^2+b^2} = \frac{a^2 + \cancel{abi} - \cancel{abi} + b^2}{a^2+b^2} = 1$$

assuming $a^2+b^2 \neq 0$ i.e. $a+bi$ is non-zero

* $\mathbb{Q}(i)$ is commutative ring with at least two elements and all non-zero elements have a multiplicative inverse

Therefore $\mathbb{Q}(i)$ is a field.

Q4:

b)

Consider the polynomial $X^2 \mp 2 \in \mathbb{Q}(i)[X]$

the root of this polynomial (assuming it exists)

Satisfies $x^2 = 2$, let $a+bi = x$, $a, b \in \mathbb{Q}$

i.e. $(a+bi)^2 = 2$

$\Rightarrow a^2 - b^2 + 2abi = 2$

equating co-efficients, we get

$\underset{①}{a^2 - b^2 = 2}, \quad \underset{②}{2ab = 0}$

② $\Rightarrow a = 0$ or $b = 0$

if $a = 0$, $-b^2 = 2$, no Solutions in $\mathbb{Q}$

if $b = 0$, $a^2 = 2$, no Solutions in $\mathbb{Q}$

i.e. $a^2 = 2, a \in \mathbb{Q}$ and $-b^2 = 2, b \in \mathbb{Q}$

are both contradictory Statements.

Therefore, the roots of $X^2 + 2$ do not exist in $\mathbb{Q}(i)$

by contradiction

Therefore, $\mathbb{Q}(i)$ is not algebraically closed.

Q5:

a) $ed \equiv 1 \pmod{44}$

$\Rightarrow 44 \mid ed - 1$

$\Rightarrow \exists k \in \mathbb{Z}$ s.t.

$44k = ed - 1$

$= 15d - 1$

i.e. $44k + 15(-d) = 1$, linear Diophantine equation

Solve using Euclids gcd algorithm

$44 = 2 \times 15 + 14$ $\qquad 1 = 15 - 1 \times (14)$

$15 = 1 \times 14 + 1$ $\longrightarrow$ $= 15 - 1 \times (44 - 2 \times 15)$ ~~ie~~ d

$14 = 14 \times 1 + 0$ $\qquad \Rightarrow 1 = 3 \times 15 - 1 \times 44$

~~Th~~ Therefore $\boxed{3}$ Satisfies $15d \equiv 1 \pmod{44}$, i.e. $\boxed{d = 3}$

b)

to decrypt Y, take $Y^d \pmod{m}$

$= Y^3 \pmod{\overset{69}{\cancel{44}}}$

Y (encrypted)	$Y^3 \pmod{\overset{69}{\cancel{44}}}$	decrypted
11	20	S
28	10	I
11	20	S
30	21	T
54	6	E
43	19	R

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

$\Rightarrow$ code Word is "SISTER"