CSE3230 Assignment A

Nathaniel De Leeuw
5283671

1

a) $\langle \mathbb{Z}_{11}^*, * \rangle = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$

We can easily know that this is a group because 11 is a prime.

We can also calculate/see that it respects all the conditions of a group (closure, associativity, ex. of identity, ex of inverse)

b) $\langle U_{11}^*, * \rangle$ see a) because 11 is prime, so also coprime with all smaller numbers $\langle Z_{11}^*, * \rangle = \langle U_{11}^*, * \rangle$

c) $\langle \mathbb{Z}_{21}^*, * \rangle = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20]\}$

Not a group $\Rightarrow$ 3 has no inverse

d) $\langle U_{21}^*, * \rangle = \{[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [19], [20]\}$

is a group, satisfy all properties

2 $\langle \mathbb{Z}_{12}, + \rangle$: $|[1]| = 12$ $|[2]| = 6$ $|[3]| = 4$ $|[4]| = 3$ $|[5]| = 12$ $|[6]| = 2$

$|[7]| = 12$ $|[8]| = 6$ $|[9]| = 4$ $|[10]| = 6$ $|[11]| = 12$

I calculated the order of every element by multiplying it and see when a multiplication is divisable by 12

$\langle \mathbb{Z}_{23}, * \rangle$: $|[1]| = 1$ $|[2]| = 11$ $|[3]| = 11$ $|[4]| = 11$ $|[5]| = 22$ $|[6]| = 11$

$|[7]| = 22$ $|[8]| = 11$ $|[9]| = 11$ $|[10]| = 22$ $|[11]| = 22$ $|[12]| = 11$

$|[13]| = 11$ $|[14]| = 22$ $|[15]| = 22$ $|[16]| = 11$ $|[17]| = 22$ $|[18]| = 11$

$|[19]| = 22$ $|[20]| = 22$ $|[21]| = 22$ $|[22]| = 2$

With Lagrang's theorem I knew that the order of the elements could only be 1, 2, 11, or 22, these

are the only dividers of 22, and 22 is the order of the group.

3

a) 71 $\phi(71) = 70$ This is because 71 is prime

b) 271 $\phi(271) = 270$ " " " 271 " "

c) 3717 $3717 = \underline{3} * 1239$

$1239 = \underline{3} * 413$

$413 = \underline{7} * \underline{59}$

the prime dividers of 3717 are 3, 7 and 59

$$\phi(3717) = 3717\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{59}\right)$$

$$= 3717 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{58}{59}$$

$$= 3 \cdot 2 \cdot 6 \cdot 58$$

$$= \boxed{2088}$$

d) 4711 $4711 = \underline{7} * \underline{673}$

$$\phi(4711) = 4711 * \frac{6}{7} * \frac{672}{673}$$

$$= 1 \cdot 6 \cdot 672$$

$$= \boxed{4032}$$

4 The 3 criterion are ① $1 \in H$, ② $ab \in H$ and ③ $a^{-1} \in H$ for all $a, b \in H$

a) No, because $[2] * [4] = [8]$ and $[8] \notin H$

b) No, because $[2] * [2] = [4]$ and $[4] \notin H$

c) No, because $[2] * [8] = [16] = [7]$ and $[7] \notin H$

d) No, because $[4] * [8] = [32] = [5]$ and $[5] \notin H$

e) No, because $[4] * [5] = [20] = [2]$ and $[2] \notin H$

5

1) Important: When we have find 1 generator, we can find the other ones by taking the generator to the power of all coprime numbers of the order of the group

a) ~~$\langle \mathbb{Z}_{11}^* \rangle$~~

b) $\langle \mathbb{Z}_{11}^* \rangle$ $\quad |\mathbb{Z}_{11}^*| = 10$, coprimes are 3, ~~4~~, ~~9~~, 7, ~~8~~, 9

1: cannot be a generator, $1^n = 1$ for all $n \geq 0$

2: $2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$

$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$

$\Rightarrow$ 2 is a generator

$\Rightarrow 2^3 = \underline{8} \bmod 11$ | 8 is a generator

$\Rightarrow 2^7 = \underline{7} \bmod 11$ | 7 is a generator

$\Rightarrow 2^9 = \underline{6} \bmod 11$ | 6 is a generator

b) $\langle \mathbb{Z}_{23}^* \rangle$ $\quad |\mathbb{Z}_{23}^*| = 22$, coprimes are

1, 3, 5, 7, 9, 13, 15, 17, 19, 21

1: NO

2: $2^0, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}$

$1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1$

$\Rightarrow$ 2 is not a generator

$\Rightarrow$ ~~$3, 5, 7, 9$~~ all those powers are also no generators

3: No ~~(see 2)~~ (power of 2)

4: No (power of 2)

~~only numbers higher than~~

~~$10, 11, 20, 8, 12, 16, 11, 9, 22, 18, 21, 13, 10, 3, 15, 6, 7$~~

5: the only possible generators are $\{5, 7, 10, 11, 14, 15, 17, 19, 23, 21, 22\}$ $\Rightarrow$ 11 numbers

These are the amount of coprime numbers with 22.

So this set needs to be the set of generators

2) $\langle 1 \rangle$ of $\langle \mathbb{Z}_{4}^{*}, \cdot \rangle$ This is an easy exercise because $\langle 1 \rangle$ has only one element, itself (1).

3) $\langle 3 \rangle$ of $\langle \mathbb{Z}_{31}^{*}, \cdot \rangle$

$n = 30$ Coprimes of 30 are $\{1, 7, 11, 13, 17, 19, 23, 29\}$

$\langle 3 \rangle = \{1, 3, 9, 27, 19, 26, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21\}$

because $\langle 3 \rangle = \langle \mathbb{Z}_{31}^{*}, \cdot \rangle$, they have the same coprimes

$\Rightarrow$ the generators are 3, 17, 13, 24, 22, 12, 11, 21.

6

$U_{28} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$

Abelian group $\Rightarrow$ LeftCoset = rightCoset

$1H = \{1, 9, 25\}$

$3H = \{3, 27, 75\} = \{3, 1, 13\}$

$5H = \{5, 45, 125\} = \{5, 17, 13\}$

$9H = \{9, 81, 225\} = \{9, 25, 1\} = 1H$

$11H = \{11, 99, 275\} = \{11, 15, 23\}$

$13H = \{13, 117, 325\} = \{13, 5, 17\} = 5H$

$15H = \{15, 135, 375\} = \{15, 23, 11\} = 11H$

$17H = \{17, 153, 425\} = \{17, 3, 5\} = 5H$

$19H = \{19, 171, 475\} = \{19, 5, 27\}$

$23H = \{23, 207, 575\} = \{23, 11, 15\} = 11H$

$25H = \{25, 225, 625\} = \{25, 1, 9\} = 1H$

$27H = \{27, 243, 675\} = \{27, 19, 3\}$

7

a) $\mathbb{Z}_{16}, * = \{0, 1, 2, 3, 4, 5\}$ $U_{14} = \{1, 3, 5, 9, 11, 13\}$

$\varphi(a+b) = 3^{a+b} = 3^a * 3^b = \varphi(a) * \varphi(b)$

It is even isomorphism because any generator g of U_n induces an isomorphism $\varphi(a) = g^a$ from U_n to $\mathbb{Z}_n$ (and the other way) with $m = \phi(n)$.

b) It is homomorphic because when we add 2 even numbers, we get an even numbers, similarly when we * positive numbers, we get a positive number (here * 1). When we add 2 odd numbers, we get an even number $(-1)*(-1) = 1$, and when we add 2 odd and an even number, we get an odd number $(-1) * 1 = -1$).

It is also epimorphic, $1 \to 1$, $2 \to 1$

$\Rightarrow$ surjective

c) $\varphi(a \cdot b) = (a \cdot b)^2 = a^2 \cdot b^2 = \varphi(a) \cdot \varphi(b)$

$\Rightarrow$ homomorphic

It is endomorphic by definition, but it is not automorphism, because negative numbers can't be mapped.

d) [illegible]

$\varphi(a+b) = a+b = \varphi(a) + \varphi(b)$

$\Rightarrow$ homomorphism

$\Rightarrow$ is also automorphism because every element is mapped to itself.

e) $\varphi(a+b) = 2(a+b) = 2a+2b = \varphi(a) + \varphi(b)$

$\Rightarrow$ homomorphism

$\Rightarrow$ endomorphism but n.t automorphism because only even numbers are mapped.

8

a) if we take the root α, we can then represent the extension field F_{2^3} in add. and mult. way.

here: $\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$

mult:	0	1	α	α^2	α^3	α^4	α^5	α^6
add:	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
vec:	000	001	010	100	011	110	111	101

b) here: $\alpha^3 = \alpha^2 + 1$

mult:	0	1	α	α^2	α^3	α^4	α^5	α^6
add:	0	1	α	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha+1$	$\alpha^2+\alpha+1$
vec:	000	001	010	100	101	111	011	110

c)

note:- the basis will not be bigger $(1, \alpha, \alpha^2, \alpha^3)$

$-\alpha^4 = \alpha + 1$

mult	0	1	α	α^1	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}
add	0	1	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha$	$\alpha^3+\alpha+1$	α^2+1	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$
vect	0000	~~0000~~ 0001	0010	0100	1000	0011	0110	1010	1011	0101	1010	0111

mult	α^{11}	α^{12}	α^{13}	α^{14}
add	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α^3+1
vect	1110	1111	1101	1001

d) If we do this, multiple multiplicative representations are going to map to the same additive representation. ~~We cannot~~ this means that it is not isomorphic anymore.

9