MATH342 Feedback and Solutions 8

1. If $a = (a_1, a_2) \in H_1 \times H_2$, then by definition of the multiplication in $H_1 \times H_2$,

$$a^n = (a_1^n, a_2^n).$$

The identity element in $H_1 \times H_2$ is $(1,1)$. Let n_1 and n_2 be the orders of a_1 and a_2 respectively. We have

$$a^n = (1,1) \quad \Leftrightarrow \quad a_1^n = 1 \wedge a_2^n = 1 \quad \Leftrightarrow n_1 \mid n \wedge n_2 \mid n$$

$$\Leftrightarrow lcm(n_1, n_2) \mid n.$$

So the order of (a_1, a_2) is $lcm(n_1, n_2)$ as required.

We have $56 = 7 \times 2^3$, and so $G_{56} \cong G_7 \times G_8$. We know that G_7 is cyclic of order $7 - 1 = 6$ (because 7 is prime) and $G_8 = \{1, 3, 5, 7\}$ with

$$3^2 \equiv 5^2 \equiv 7^1 \equiv 1 \mod 8.$$

So the elements of G_8 are all of order 2, apart from 1 which is of order 1 and the possible orders of the elements of the cyclic group G_7 are the divisors of 6, that is,

$$1, \quad 2, \quad 3, \quad 6.$$

Applying question 1 to the product $G_7 \times G_8$, the possible orders of elements of G_{56} are exactly the same.

Note that the answer to this question is nothing *to do with the divisors of* 56 *– because the orders of elements of* G_7 *are the divisors of* 6*, not* 7*. It also may be a bit surprising that evey element of* G_8*, apart from* 1*, has order* 2 *– there are no elements of order* 4*.*

2.

a) $x^4 \equiv 1 \mod 5$ for all $x \in \mathbb{Z}_5^*$. So $x^4 - 1$ is divisible by $x - 1$, $x - 2$, $x - 3$ and $x - 4$ in $\mathbb{Z}_5[x]$ and

$$x^4 - 1 = (x-1)(x-2)(x-3)(x-4).$$

b) By inspection $1^2 + 1 + 1 \equiv 0 \mod 3$ so $x - 1 \equiv x + 2$ must be a factor. Again by inspection we see that $x^2 + x + 1 = (x+2)^2 \mod 3$.

3. The prime factorisations are

$$37 = 37, \; 38 = 2 \times 19, \; 40 = 2^3 \times 5, \;\; 41 = 41, \; 44 = 2^2 \times 11, \;\; 45 = 3^2 \times 5.$$

- We have $37 \equiv 1 \mod 4$ and $37 = 6^2 + 1$.
- Since $19 \equiv 3 \mod 4$, 38 does not satisfy the necessary condition for being a sum of two integer squares. In any case if $38 = a^2 + b^2$ then one of a and b has to be ± 5 or ± 6, because $4^2 = 16 < 38/2 = 19$ and $7^2 > 38$. But $38 - 6^2 = 2$ and $38 - 5^2 - 13$, and neither 2 nor 13 is a square of an integer.
- We have $5 \equiv 1 \mod 4$ and $40 = 6^2 + 2^2$.
- We have $41 \equiv 1 \mod 4$ and $41 = 5^2 + 4^2$
- We have $11 \equiv 3 \mod 4$. In any case, if $44 = a^2 + b^2$ then, once again one of a and b has to be ± 5 or ± 6. But neither $44 - 25 = 19$ nor $44 - 36 = 8$ is the square of an integer.

- We have $5 \equiv 1 \mod 4$ and $45 = 6^2 + 3^2$.

In the case of 38 *and* 44*, I wanted to see a direct proof that the number was not a sum of two integer squares.*

4.

$$x^3 - 1 = (x-1)(x^2+x+1), \qquad x^4 - 1 = (x-1)(x+1)(x^2+1),$$
$$x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1),$$
$$x^{12} - 1 = (x^6-1)(x^6+1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1)$$

In each case these polynomials are irreducible in $\mathbb{Z}[x]$ because ± 1 are not zeros of the three quadratics x^2+1, x^2+x+1 and x^2-x+1. In fact those three quadratics do not have any real roots.

Now we show that $x^4 - x^2 + 1$ is irreducible in $\mathbb{Z}[x]$. Once again, ± 1 is not a zero of this polynomial. So if this polynomial is not irreducible, it must factorise as a product of two quadratics with integer coefficients. Because the coefficients of x^4 is 1 and the constant term is 1, and because the coefficients of x and x^3 are 0, we would have

$$x^4 - x^2 + 1 = (x^2+ax+1)(x^2-ax+1) \quad \text{or} \quad x^4 - x^2 + 1 = (x^2+ax-1)(x^2-ax-1).$$

Then the coefficient of x^2 on the right-hand side is $-a^2-2$ or $-a^2+2$, which has to be equal to 1, that is, we need $a^2 = -1$ or $a^2 = 3$. Both of these are impossible for $a \in \mathbb{Z}$.

Using the inductive definition

$$x^n - 1 = \prod_{d \min n,\ d \geq 1} \psi_d(x)$$

the cyclotomic polynomials are

$$\psi_3(x) = x^2+x+1, \quad \psi_4(x) = x^2+1, \quad \psi_6(x) = x^2-x+1, \quad \psi_12(x) = x^4-x^2+1.$$

It is not part of the definition that the cyclotomic polynomials are irreducible in $\mathbb{Z}[x]$ *– although it is a theorem (not proved in this course) that they are.*

5.

a) We have

$$c_1^2 = \left(c_1 + \frac{1}{2}\right)^2 - (c_1 + \frac{1}{2}) + \frac{1}{4}$$

and similarly for c_2. So there is an integer n such that

$$c_1^2 - c_2^2 = n + \frac{1}{4} - \frac{5}{4} = n - 1 \in \mathbb{Z}.$$

b) Since $c = c_1 + c_2\sqrt{5}$ divides n in $\mathcal{O}[\sqrt{5}]$, there is $d \in \mathcal{O}[\sqrt{5}]$ such that $n = cd$. Then $\theta(n) = \theta(c)\theta(d)$. But $\theta(n) = n$ and $\theta(c) = c_1 - c_2\sqrt{D}$. So since $\theta(d) \in \mathcal{O}[\sqrt{5}]$, we see that $c_1 - c_2\sqrt{5}$ divides n.

c) Now $c = c_1 + c_2\sqrt{5}$ is a unit if and only if there exists $d \in \mathcal{O}[\sqrt{5}]$ with $cd = 1$. But

$$1 = \theta(1) = \theta(cd) = \theta(c)\theta(d).$$

So c is a unit if and only if $\theta(c) = c_1 - c_2\sqrt{5}$ is. So if c is a unit then, for d as above

$$1 = cd\theta(c)\theta(d) = (c_1^2 - 5c_2^2)d\theta(d).$$

So since $d\theta(d)$ is an integer, it must be the case that $c_1^2 - 5c_2^2 = \pm 1$. Conversely, if $c_1^2 - 5c_2^2 = \pm 1$ then $(c_1 + c_2\sqrt{5})(\pm(c_1 + c_2\sqrt{5})) = 1$ and $c_1 + c_2\sqrt{5}$ is a unit.