412 Individual HW1

Jack Madden

Februrary 2024

Problem 1

a)

b) A ring homomorphism contains a group homomorphism between the groups induced by the additive operation. Since the image of a homomorphism is a subgroup, and the only finite subgroup in $\mathbb{Q}$ is the trivial group, the only homomorphism from a finite ring to a finite subgroup of $\mathbb{Q}$ will be the trivial one, mapping all elements in $\mathbb{Z}_5$ to the identity.

c)

Problem 2

a) This is indeed a subring. We will show closure under addition, existence of additive identity and inverses, and closure under multiplication. Choosing $a, b = 0$ gives the additive identity, inverse also exist as for any a, b, simply choose $a, b \in \mathbb{Z}$. Closure under addition ($a, b, c, d \in \mathbb{Z}$):

$$a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2}$$

Closure under multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$$

b) This is a subring, as it contains the additive identity $e(x) = 0$, as $e(3) = 0$, is closed under addition, as for any $f, g \in S$, $(f + g)(3) = f(3) + g(3) = 0 + 0 = 0$, and is also closed under multiplication, as for $f, g \in S$, $(f \cdot g)(3) = f(3) \cdot g(3) = 0 \cdot 0 = 0$. Additive inverses are also in S, as for any $f \in S$, $-f(3) = -(f(3)) = -0 = 0$.

Problem 3

a) $(1, 1), (1, 3), (3, 1), (3, 3)$. These are all the ordered pairs containing only integers relatively prime to 4.

b) These are:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Problem 4

Take $S = \{0, 3\} \in (\mathbb{Z}_6, +, \cdot)$. It has unity $3 \neq 1$ as $3 \cdot a = a$ for all $a \in S$.

Problem 5

To show that the set of all units in a ring with unity is a group under multiplication, we must show that it contains the multiplicative identity, that every element has an inverse, and that the operation is associative. $(U, \cdot)$ contains the unity as the unity is a unit, as it is its own inverse. Let $a \in U$. We will now show that this implies $a^{-1} \in U$. a^{-1} is a unit as it has an inverse a, and is therefore also in U. Finally, the binary operation is associative, as we have that the multiplication is associative from the fact that it descends from a ring.

Problem 6

First we will prove reflexivity. Clearly, a ring is isomorphic to itself under the map $\phi(x) = x$, as for any x, y in a ring R, $x + y = \phi(x) + \phi(y) = \phi(x + y) = x + y$. This map is also a bijection, namely the identity bijection.

Next, we will prove symmetry. Let R be isomorphic to S under the map ϕ. Then we also have that S is isomorphic to R under the map ϕ^{-1}. We know this map exists as ϕ is a bijection.

Finally, we will show transitivity. Let R be isomorphic to S under ϕ and let S be isomorphic to T under ψ. We then have that $\phi \cdot \psi$ is an isomorphism between R and T.

Problem 7

a) We have that $2022 = 2 \cdot 3 \cdot 337$. For a power of $x \in \mathbb{Z}_{2022}$ to be 0 mod 2022, it would have to contain all of the prime factors. However, since no prime factor is repeated in this factorization, no number less than 2022 has these prime factors.

b) $(\mathbb{Z}_4, +, \cdot)$ has nilpotents 0 and 2. This is because the product of two odd numbers will always be odd, which can be extended recursively to show that there is no n such that 1^n or 3^n is even, and further divisible by 4.

c) We have that $x^m = 0, y^n = 0$ for some $m, n > 0$. We can show that $x+y$ is nilpotent by showing that $(x + y)^{m+n} = 0$.

$$(x+y)^{m+n} = x^m x^n + x^m x^{n-1} y + x^m x^{n-2} y^2 + \cdots + x^m y^n + x^{m-1} y^n y + x^{m-2} y^n y^2 + \cdots + y^n y^m$$

We then observe that in each term, there will be at least one factor $x^m = y^n = 0$ which will make each term go to zero and consequently the whole sum is zero. Thus we have shown that if x, y are nilpotent, then their sum is also nilpotent.

Problem 8

a) 1 and 2 are the solutions in $\mathbb{Z}_5$.

b) No solutions are in $\mathbb{Z}_7$.

c) No solutions are in $\mathbb{Z}_8$.

Problem 9

If the characteristic is zero, done.
Otherwise, suppose it is some positive n. We will perform a proof by contradiction to show that n must be prime. Let $n = km, k, m > 1$. We show that either $k \cdot 1 = 0$ or $m \cdot 1 = 0$. If $k \cdot 1 = 0$, we are done. Otherwise, let $k \cdot 1 = \ell \neq 0$. Then

$$n \cdot 1 = m \cdot (k \cdot 1) = m \cdot \ell = \underbrace{\ell + \cdots + \ell}_{\text{m times}} = \ell \left(\underbrace{1 + \cdots + 1}_{\text{m times}} \right) = 0$$

We have that $\ell \neq 0$, and by the fact that an integral domain has no zero divisors, this implies that $m \cdot 1 = 0$. Essentially what we have shown now is that for any supposed "composite characteristic" of integral domain, it can keep being factored until it is prime, where you will have the minimal n.

Problem 10

a) No, this is not an integral domain, as it has divisors of zero. For example $43 \cdot 47 = 0$ in this ring. Since it is not an integral domain, it is also not a field.

b) Integral domains are subsets of commutative rings with unity. The even integer ring does not have a unity, so it is not a commutative ring with unity and therefore cannot be an integral domain, and therefore not a field.

c) This is not a field, as not every element is a unit. Take $x \in R$, its multiplicative inverse is x^{-1} which is not in R. However, it is an integral domain. We can see that for $a, b \in R$, if a and b are not zero, then $a \cdot b$ will not be zero as we observe there will always be a nonzero term x^{m+n} where m and n are the degrees of a and b respectively.

d) Complex numbers are a field. This is because every non-zero complex number has a multiplicative inverse, for $C = a + bi$, its inverse is $\frac{a-bi}{a^2+b^2}$. We also have that in a commutative ring with unity, every element is either a zero divisor or a unit.

   Proof: Let $a \neq 0$ be a zero divisor and also a unit. Thus there exist a^{-1} such that $aa^{-1} = 1$, and $b \neq 0$ such that $ab = 0$. Then

$$ab = 0$$
$$a^{-1}ab = 0$$

   But then:

$$1 \cdot b = 0$$

   which implies b must be 0, contradiction.

   Thus, as we have shown every nonzero element has an inverse, this implies that there are no zero divisors and therefore $\mathbb{C}$ is a field.