Math 320 Take Home Final Key

May 2, 2024

1.

$$\{(0,e),(0,r),\left(0,r^2\right),(0,f),(0,fr),\left(0,fr^2\right),(1,e),(1,r),\left(1,r^2\right),(1,f),(1,fr),\left(1,fr^2\right),(2,e),(2,r),\left(2,r^2\right),(2,f),(2,fr),\left(2,fr^2\right)\}$$

2.

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$$

3.

We need to show ϕ is one-to-one, onto, and obeys the homomorphism property. Suppose $x, y \in G$

One-to-one

Suppose $\phi(x) = \phi(y)$. Then

$$\sqrt{x} = \sqrt{y}$$

so

$$\sqrt{x}^2 = \sqrt{y}^2$$

and thus

$$x = y$$

Onto

Let $x \in \mathbb{R}^+$. Then $x^2 \in \mathbb{R}^+$, and as $\phi\left(x^2\right) = \sqrt{x^2} = x$, then x is onto.

Homomorphism

Let $x, y \in G$. Then $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$

4.

$$2x^2 + ix + (1-i) = (x+1)(2x + (-2+i)) + (3-2i)$$

5.

$$\left(x^3+4x+3\right)\left(4x^3+2x^2+1\right)$$

$$= 4x^6 + 2x^5 + x^3 + 16x^4 + 8x^3 + 4x + 12x^3 + 6x^2 + 3 = 4x^6 + 2x^5 + 16x^4 + 21x^3 + 6x^2 + 4x + 3$$

but as we are working in $\mathbb{Z}_7[x]$,

$$= 4x^6 + 2x^5 + 2x^4 + 0x^3 + 6x^2 + 4x + 3 = 4x^6 + 2x^5 + 2x^4 + 6x^2 + 4x + 3$$

6.

Let's show each of the ring axioms. Throughout the entire proof, let $f, g, h \in E$.

Closure

$$(f+g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f+g)(x)$$

$$(f*g)(-x) = f(-x)\, g(-x) = f(x)\, g(x) = (fg)(x)$$

Additive Identity

Consider $f(x) = 0$. Then $f(x) = 0 = f(-x)$. As

$$(g+0)(x) = g(x) + 0 = g(x)$$

then we have 0 as the additive identity.

Additive Inverses

Consider $-f(x)$. Then

$$-f(-x) = -f(x)$$

and

$$(f + -f)(x) = f(x) + -f(x) = 0$$

so we have additive inverses.

Associativity of Addition

Consider

$$((f+g)+h)(x) = (f+g)(x) + h(x) = f(x) + g(x) + h(x)$$

$$= f(x) + (g+h)(x) = (f+(g+h))(x)$$

Commutativity of Addition

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$$

Associativity of Multiplication

$$((fg)\, h)(x) = (fg)(x)\, h(x) = f(x)\, g(x)\, h(x)$$

$$f(x)\,(gh)(x) = (f\,(gh))(x)$$

Distributive Laws

$$((f+g)\, h)(x) = (f+g)(x)\, h(x) = (f(x) + g(x))\, h(x)$$

$$= f(x)\, h(x) + g(x)\, h(x) = (fh)(x) + (gh)(x)$$

Similarly:

$$(f\,(g+h))(x) = f(x)\,(g+h)(x) = f(x)\,(g(x) + h(x))$$

$$= f(x)\, g(x) + f(x)\, h(x) = (fg)(x) + (fh)(x)$$

Thus $(R, +, *)$ is a ring.

7.

For convenience, call $R = \mathbb{Q}[x]\ \langle x^2 - n\rangle = I$ and $\mathbb{Q}[x] / \langle x^2 - n\rangle = R/I$

a)

Let's use the ideal test! We need to show I is nonempty and that for any $f(x), g(x) \in I$ that $f(x) - g(x) \in I$ and for any $h(x) \in R$ and $f(x) \in I$ that $f(x)h(x), h(x)f(x) \in I$. Suppose $f(x), g(x) \in I$. Then

$$f(x) = r(x)\left(x^2 - n\right), g(x) = q(x)\left(x^2 - n\right)$$

for some $p(x), q(x) \in R$. Thus

$$f(x) - g(x) = p(x)\left(x^2 - n\right) - q(x)\left(x^2 - n\right) = (p(x) - q(x))\left(x^2 - n\right) \in I$$

and $r(x), q(x) \in R$. If we use $f(x)$ as above, and have $h(x) \in R$, then

$$f(x)h(x) = p(x)\left(x^2 - n\right)h(x) = (p(x)h(x))\left(x^2 - n\right)$$

and as $p(x)h(x) \in R$, then $f(x)h(x) \in I$. As R is a commutative ring, then $h(x)f(x) = f(x)h(x) \in I$. Finally, to show I is nonempty, note that $x^2 - n \in I$

b)

Consider the mapping $\phi(a + bx + I) = a + b\sqrt{n}$. To show this is an isomorphism, we will show this function is one-to-one, onto, and satisfies both homomorphism properties.

One-to-One

Suppose $\phi(a + bx + I) = \phi(c + dx + I)$. Then

$$\phi(a + bx + I) = a + b\sqrt{n} = c + d\sqrt{n} = \phi(c + dx + I)$$

As $a, b, c, d \in \mathbb{Q}$ and $\sqrt{n} \notin \mathbb{Q}$, then

$$a = c, b = d$$

and

$$a + bx + I = c + dx + I$$

Onto

Suppose $a + b\sqrt{n} \in R$. Then

$$\phi(a + bx + I) = a + b\sqrt{n}$$

for $a + bx + I \in R$

Homomorphisms

Let $a + bx + I, c + dx + I \in R$. Then

$$\phi(a + bx + I + c + dx + I) = \phi((a + c) + (b + d)x + I)$$

$$= a + c + (b + d)\sqrt{n} = \left(a + b\sqrt{n}\right) + \left(c + d\sqrt{n}\right) = \phi(a + bx + I) + \phi(c + dx + I)$$

Similarly,

$$\phi((a + bx + I)(c + dx + I)) = \phi\left(ac + (ad + bc)x + bdx^2 + I\right)$$

but as $I = \langle x^2 - n \rangle$, then

$$ac + (ad + bc)\,x + bdx^2 + I = ac + (ad + bc)\,x + bdx^2 + -bd\left(x^2 - n\right) + I$$

$$= (ac + bdn) + (ad + bc)\,x + I$$

Thus

$$\phi\left(ac + (ad + bc)\,x + bdx^2 + I\right) = \phi\left((ac + bdn) + (ad + bc)\,x + I\right)$$

$$= ac + bdn + (ad + bc)\sqrt{n} = \left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right)$$

8.

As $\mathbb{Q}$ is an integral domain, then $\mathbb{Q}[x]$ is an integral domain. As we are taking the quotient ring of an integral domain, we know $I = \langle x^2 - n \rangle$ is a prime (maximal) ideal if $R/I = \mathbb{Q}[x] / \langle x^2 - n \rangle$ is an integral domain (field).

Perfect Square

Suppose $n = m^2$ for some $m \in \mathbb{Z}$. Then

$$x^2 - n = x^2 - m^2 = (x - m)(x + m) \in I$$

and as $(x - m), (x + m) \in \mathbb{Q}[x]$ but $(x - m), (x + m) \notin I$. But

$$((x - m) + I)((x + m) + I) = (x - m)(x + m) + I = I$$

thus R/I is not an integral domain and thus not a field.

Not a Perfect Square

Suppose n is not a perfect square. Then by **7b)**,

$$R/I \approx \mathbb{Q}\left[\sqrt{n}\right]$$

Let's show $F = \mathbb{Q}[\sqrt{n}]$ is a field. We already know this is a ring, so all the remains to be shown is that F is commutative under multiplication, has no zero divisors, F has a unity, and every nonzero element is a unit. Throughout the proof, we will use $a + b\sqrt{n}, c + d\sqrt{n} \in F$ for convenience.

Commutativity Under Multiplication

$$\left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right) = ac + bdn + (ad + bc)\sqrt{n} = ca + dbn + (da + cb)\sqrt{n} = \left(c + d\sqrt{n}\right)\left(a + b\sqrt{n}\right)$$

Alternatively, since R is a commutative ring, then so is R/I.

No Zero Divisors

Suppose

$$\left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right) = 0$$

Suppose WLOG that $(a + b\sqrt{n}) \neq 0$. Then

$$\left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right) = ac + bdn + (ad + bc)\sqrt{n} = 0$$

so

$$(ac + bdn), (ad + bc) = 0$$

From $(ad+bc)=0$,

$$a=-\frac{bc}{d}$$

so

$$ac+bdn=-\frac{bc}{d}c+bdn=0$$

so

$$bdn=\frac{bc^2}{d}$$

$$bd^2n=bc^2$$

$$d^2n=c^2$$

$$d\sqrt{n}=c$$

but as $c,d\in\mathbb{Q}$ but $\sqrt{n}\notin\mathbb{Q}$, then $d\sqrt{n}\notin\mathbb{Q}$ and thus this equality can only hold if $c=d=0$.

Unity

Consider $1\in R$. Then $1+I\in R/I$. For any $a+I\in R/I$, we have

$$(1+I)(a+I)=1a+I=a+I$$

so $1+I$ is a unity in R/I. Alternatively, as R is a ring with unity, so is R/I.

Units

Suppose $a+b\sqrt{n}\neq 0$. Then

$$1=\frac{a+b\sqrt{n}}{a+b\sqrt{n}}*\frac{a-b\sqrt{n}}{a-b\sqrt{n}}=\left(a+b\sqrt{n}\right)\frac{a-b\sqrt{n}}{a^2-b^2n}=\left(a+b\sqrt{n}\right)\left(\left(\frac{a}{a^2-b^2n}\right)+\left(\frac{-b}{a^2-b^2n}\right)\sqrt{n}\right)$$

so $\left(a+b\sqrt{n}\right)^{-1}=\left(\left(\frac{a}{a^2-b^2n}\right)+\left(\frac{-b}{a^2-b^2n}\right)\sqrt{n}\right)$. As all conditions are met, then R/I is a field.

a)

This is true when n is not a perfect square.

b)

This is true when n is not a perfect square.

9.

a)

First, let's show H this is a subgroup. We can apply one of the subgroup tests. First, let's show H is nonempty.

$$1\in H$$

Now, let's apply the second subgroup test. Suppose $a,b\in H$. Then $|a|=|b|=1$. Further,

$$\left|ab^{-1}\right|=\left|\frac{a}{b}\right|=\frac{|a|}{|b|}=\frac{1}{1}=1$$

So $ab^{-1}\in H$. As the complex numbers are commutative under multiplication, then G is abelian. All subgroups of an abelian group are normal. Thus H is a normal subgroup of G.

b)

Consider the mapping $\phi(aH) = |a|$. To show this is an isomorphism, we need to show this is one-to-one, onto, and a homomorphism.

One-to-One

Suppose $\phi(aH) = \phi(bH)$. Then

$$|a| = |b|$$

Consider

$$\left|ab^{-1}\right| = \frac{|a|}{|b|} = \frac{|a|}{|a|} = 1$$

thus

$$ab^{-1} \in H$$

and thus $aH = bH$.

Onto

Suppose $a \in \mathbb{R}^+$. Then

$$a = |a| = \phi(aH)$$

Homomorphism

Consider

$$\phi((aH)(bH)) = \phi((ab)H) = |ab| = |a||b| = \phi(aH)\phi(bH)$$

Thus $G/H \approx (\mathbb{R}^+, *)$

10.

We can use the subring test. We need to show S, the set of all nilpotent elements satisfied the subring test. For convenience, suppose $x, y \in S$ throughout this proof such that $x^n = 0, y^m = 0$.

Non-Empty

Consider $0 \in R$. $0^2 = 0$

Difference

We need to show $x - y \in S$. Consider

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} c_k x^k (-y)^{n+m-k}$$

where $c_k = \begin{pmatrix} n+m \\ k \end{pmatrix}$ is the binomial coefficient. But as either $k \geq n$ or $n+m-k \geq m$ for each $0 \leq k \leq n+m$, then either $x^k = 0$ or $y^{n+m-k} = 0$ for each k, thus

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} (-1)^{n+m-k} c_k x^k y^{n+m-k} = \sum_{k=0}^{n+m} c_k 0 = 0$$

Thus $x - y \in S$

Product

We need to show $xy \in S$. Then

$$(xy)^n = xy \dots xy = x^n y^n = 0y^n = 0$$

as R is a commutative ring. Thus $xy \in S$ and S is a subring of R.

11.

Suppose $a^2 = a$ and ϕ is a ring homomorphism. Then

$$\phi(a)^2 = \phi\left(a^2\right) = \phi(a)$$

so $\phi(a)$ is idempotent.

12.

No comment.