

Fall 2007

Elementary Abstract Algebra I Practise Final

Name: _____

1	2	3	4	5	6	7	8	TOT.

FINAL EXAM: 15:15–17:05 THURSDAY OF FINALS WEEK.

The real final will look roughly like this, probably slightly shorter questions, but similar topics.

Sections to revise: Chapter 1 (all), Section 2.1, Chapter 4 (all), Section 5.1, Definition 5.2.1 (why is it automatic that $\phi(1) = 1$ if ϕ is one-to-one and onto?).

Then go over all homeworks and make sure you understand how to do them with hindsight!

Revising is a key part of learning mathematics: lots of things you didn't completely understand the first time round should be easier when you go back over it again!!

1. Let F be a field and $f(x) \in F[x]$ be an irreducible polynomial. Prove carefully that $f(x)|a(x)b(x)$ implies either $f(x)|a(x)$ or $f(x)|b(x)$.

Say $f(x) \nmid a(x)$.

Then as $f(x)$ is irreducible, $\text{GCD}(f(x), a(x)) = 1$

$$\therefore 1 = f(x)p(x) + a(x)q(x)$$

$$\therefore b(x) = \underbrace{f(x)p(x)b(x)}_{f(x) \text{ divides}} + \underbrace{a(x)b(x)q(x)}_{f(x) \text{ divides}} \Rightarrow f(x) \parallel b(x)$$

2. (a) For which values of $a = 1, 2, 3, 4$ is $\mathbb{Z}_5[x]/\langle x^2 + x + a \rangle$ a field? Explain.

It's a field $\Leftrightarrow x^2 + x + a$ has no roots in \mathbb{Z}_5

$$a=1: x^2 + x + 1 \quad \checkmark \quad \text{field}$$

$$a=2: x^2 + x + 2 \quad \checkmark \quad \text{field}$$

$$a=3: x^2 + x + 3 \quad x=1 \text{ a root} \quad \times$$

$$a=4: x^2 + x + 4 \quad x=2 \text{ a root} \quad \times$$

(b) For which values of $k = 2, 3, 4, 5$ is $\mathbb{Z}_k[x]/\langle x^2 + x + 1 \rangle$ a field? Explain (and be extra careful with $k = 4$).

Assume $k \neq 4$ It's a field $\Leftrightarrow x^2 + x + 1$ has no roots in \mathbb{Z}_k

So k is prime!

$$k=2: x^2 + x + 1 \quad \checkmark \quad \text{field}$$

$$k=3: x=1 \text{ a root} \quad \times$$

$$k=5: \checkmark \text{ field (see (a))}$$

If $k=4$ \mathbb{Z}_4 is not a field $\therefore \mathbb{Z}_4[x]/\langle x^2 + x + 1 \rangle$ is certainly not

(eg $2 \times 2 = 0$... non-zero zero divisor
 $\dots 2$ cannot be a unit!)

3. Factor the polynomial $x^9 - 1$ completely into irreducibles in the ring $\mathbb{Q}[x]$. Use Eisenstein's criterion to prove that each of your irreducible factors really are irreducible.

$$x^3 - 1 = (x-1)(x^2 + x + 1) \quad \text{substitute } x \rightarrow x^3$$

$$\therefore x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$$

$$= (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

$\underbrace{(x-1)}_{\text{irred as linear}}$ $\underbrace{(x^2 + x + 1)}_{\text{irred as roots are } -\frac{1 \pm \sqrt{3}i}{2} \notin \mathbb{Q}}$ $\underbrace{(x^6 + x^3 + 1)}_{\text{irred}}$

→ Set $x = y + 1$

$$(y+1)^6 + (y+1)^3 + 1 =$$

$$y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3$$

which is irreducible by Eisenstein's criterion, $p=3$.

1	6	15	21	18	9	3
		13	3			
					1	
<hr/>						
1	6	15	21	18	9	3

4. (a) Let F be a field and $f(x) \in F[x]$ be a polynomial. Prove the remainder theorem:

"For $a \in F$, $(x - a)$ is a linear factor of $f(x)$ if and only if $f(a) = 0$."

(\Rightarrow) If $f(x) = (x-a)g(x)$ then $f(a) = (a-a)g(a) = 0$ ✓

(\Leftarrow) Suppose $f(a) = 0$.

Use division algorithm to divide:

$f(x) = (x-a)g(x) + r$ ← zero or non-zero, deg < 1
 $\therefore r$ is a constant!

Let $x = a$

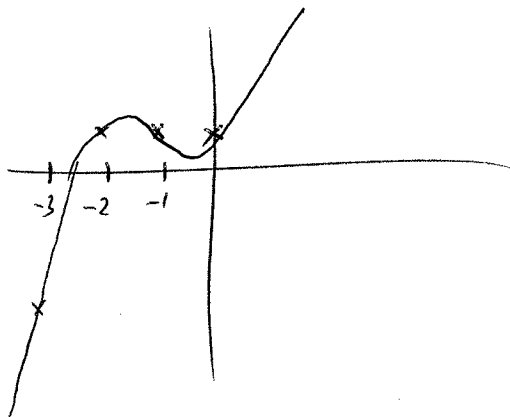
$0 = f(a) = (a-a)g(a) + r = r$

$\therefore r = 0$

$\therefore f(x) = (x-a)g(x)$ so $(x-a)$ is a linear factor

(b) Prove that $f(x) = x^3 + 3x^2 + 2x + 1$ is irreducible over \mathbb{Q} . (Hint: draw a rough sketch of the graph by plotting points at $x = -3, -2, -1$ and 0 and use a recent theorem about rational roots...)

Cubic



No integer roots - clear from graph!

By theorem, a monic poly with integer coefficients has only integer roots or irrational roots

\therefore No roots in \mathbb{Q}

As its a cubic this shows its irreducible over \mathbb{Q}

5. (a) Prove for any $x \in \mathbb{Z}$ that $x^5 \equiv x \pmod{5}$.

$$0^5 \equiv 0 \pmod{5} \checkmark$$

$$1^5 \equiv 1 \pmod{5} \checkmark$$

$$2^5 = 32 \equiv 2 \pmod{5} \checkmark$$

$$3^5 = 9 \cdot 9 \cdot 3 \equiv -1 \cdot -1 \cdot 3 \equiv 3 \pmod{5} \checkmark$$

$$4^5 = (-1)^5 \equiv -1 \equiv 4 \pmod{5} \checkmark$$

Done! Because for any $x \in \mathbb{Z}$

$$x^5 - x \equiv [x]^5 - [x] \pmod{5} \therefore \text{Only need to consider}$$

(b) Find the multiplicative inverse of x in $\mathbb{Z}_5[x]/\langle x^{2007} + 2 \rangle$.

$x = 0, 1, 2, 3$ and 4 !!

$$[x^{2007} + 2] = 0$$

$$\therefore [2x^{2007} - 1] = 0$$

$$\therefore [1] = [2x^{2007}] = [2x^{2006}] \cdot [x]$$

$$\therefore [x]^{-1} = [2x^{2006}]$$

← You could use the Euclidean algorithm but this trick is easier (only works for $[x]^{-1}$)

(c) Is the ring $\mathbb{Z}_5[x]/\langle x^{2007} + 2 \rangle$ a field?

If it was it would be a really hard question, so it had better not be.

Try looking for a root $x=2$?

Quicker

For $x \neq 0$

$$x^4 \equiv 1 \pmod{5}$$

$$\begin{aligned} 2^{2007} &= (2^5)^{400} \cdot 2^3 = 2^{400} \cdot 2^3 = (2^5)^{80} \cdot 2^3 = 2^{80} \cdot 2^3 = (2^5)^{16} \cdot 2^3 \\ &= 2^4 = 2^5 \cdot 2^5 \cdot 2^5 = 2^4 = 2^7 = 8 \end{aligned}$$

$$\therefore x^{2007} \equiv x^3 = 8$$

Reduce 2007 mod 4

$$\therefore 2^{2007} + 2 \equiv 8 + 2 \equiv 0 \pmod{5}$$

\therefore It has a linear factor

NOT a field

7. For each of the following, decide whether the function is *well-defined*, and if so determine whether it is *one-to-one* and/or *onto*.

(a) $f: \mathbb{C} \rightarrow \mathbb{C}, x + iy \mapsto 2y + i(\frac{\sqrt{3}}{2}x - y)$. Obviously well-defined

$g: \mathbb{C} \rightarrow \mathbb{C}, u + iv \mapsto i\frac{u}{2} + \frac{2}{\sqrt{3}}(v + \frac{u}{2})$ is a 2-sided inverse

$\therefore f$ is 1-1 and onto.

~~is a 2-sided inverse~~

(b) $f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_8, [x]_4 \mapsto [3x]_8$.

Not well-defined $\left(\begin{array}{l} [0]_4 \mapsto [0]_8 \\ [4]_4 \mapsto [12]_8 \end{array} \right)$

(c) $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}, (x, y) \mapsto x + iy$.

Obviously well-defined, 1-1 and onto.

(d) $f: \mathbb{R} \rightarrow \mathbb{C}, x \mapsto x^2 + ix$.

Obviously well-defined

$g: \mathbb{C} \rightarrow \mathbb{R}, u + iv \mapsto v$ is left inverse $g(f(x)) = x$

$\therefore f$ is 1-1. It's not onto, eg 1 is not in image of f

(e) $f: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}, (x, y) \mapsto (x^2, x + y)$.

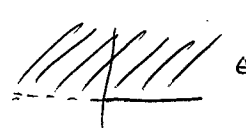
$(1, -1) \mapsto (1, 0)$
 $(-1, 1) \mapsto (1, 0) \therefore$ Not 1-1

only get stuff whose real part is the square of its imaginary part!

It is onto: $g: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}$

$(u, v) \mapsto (\sqrt{u}, v - \sqrt{u})$
 is a right inverse $f(g(u, v)) = (u, v)$

choose the \sqrt{u} in the region shaded so unambiguous!



8. Here are five rings. Work out which of them are isomorphic to each other.

Explain!

$R_1 = \mathbb{Z}_2[x]/\langle x^3 + x \rangle$. \leftarrow has additive order 2, not a field
 $R_2 = \mathbb{Z}_8$ \leftarrow has ~~mult~~ additive order 8, not a field
 $R_3 = \mathbb{Z}_2 \times \mathbb{Z}_4$. \leftarrow has additive order 4, not a field
 $R_4 = \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ \leftarrow a field
 $R_5 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. \leftarrow has additive order 2, not a field

$\therefore R_2, R_3, R_4, R_5$ all different.

Maybe $R_1 \cong R_5$.

In fact it is ~~use CRT~~

~~$x^3 + x = x(x^2 + 1)$ \leftarrow relatively prime~~

~~$\therefore \mathbb{Z}_2[x]/\langle x^3 + x \rangle \cong \mathbb{Z}_2[x]/\langle x \rangle \times \mathbb{Z}_2[x]/\langle x^2 + 1 \rangle$~~

~~$x^2 + 1 = (x+1)^2$ \leftarrow \mathbb{Z}_2~~

No it is not!!! They are all different!

In R_5 is there any element of multiplicative order 2?

If $(x, y, z)^2 = (1, 1, 1)$ then $x^2 = y^2 = z^2 = 1$ so $x = y = z = 1$

so $(x, y, z) = (1, 1, 1)$ already. NO elts of order 2

In R_1 there are elements of multiplicative order 2

$$\begin{aligned} \text{eg } (x^2 + x + 1)^2 &= x^4 + x^2 + 1 + 2x^3 + 2x^2 + 2x = x^4 + x^2 + 1 \\ &= 2x^2 + 1 = 1 \end{aligned}$$