

Winter 2008

Elementary Abstract Algebra II Practise Final

Name: \_\_\_\_\_

1	2	3	4	5	6	7	8	TOT.

FINAL EXAM: 15:15-17:05 TUESDAY OF FINALS WEEK.

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

Sections to revise: Well everything, of course, but pay special attention to 5, 9 and 6.1-6.3. Try to read through all the \*short\* proofs from your notes as you know I expect you to be able to reproduce some of these. Try to learn definitions \*precisely\*.

1. Let  $u = \sqrt[3]{2}$ . Express  $(1 + u^2)^{-1}$  in the form  $a + bu + cu^2$  for  $a, b, c \in \mathbb{Q}$  in two different ways:

(a) by solving the equation  $(a + bu + cu^2)(1 + u^2) = 1$ ;

$$a + bu + cu^2 + au^2 + bu^3 + cu^4 = 1 \quad u^3 = 2$$

$$\begin{cases} a + 2b = 1 \\ b + 2c = 0 \\ a + c = 0 \end{cases} \quad \therefore \begin{cases} b = \frac{2}{5} \\ c = -\frac{1}{5} \\ a = \frac{1}{5} \end{cases} \quad \boxed{\frac{1}{5} + \frac{2u}{5} - \frac{1}{5}u^2}$$

(b) by using the Euclidean algorithm to write  $\text{GCD}(x^2 + 1, x^3 - 2)$  as a linear combination of  $x^2 + 1$  and  $x^3 - 2$  then reducing modulo  $x^3 - 2$ .

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

$$x^2 + 1 = (x-2)(x+2) + 5$$

$$5 = x^2 + 1 - (x-2)[x(x^2 + 1) - (x^3 - 2)] = (x^2 + 1)(1 - x(x-2)) + (x-2)(x^3 - 2)$$

$$\therefore (x^2 + 1)^{-1} \equiv \frac{1}{5} (1 - x(x-2)) \pmod{x^3 - 2}$$

$$\equiv \frac{1}{5} + \frac{2}{5}x - \frac{1}{5}x^2$$

$$\boxed{\frac{1}{5} - \frac{2u}{5} + \frac{1}{5}u^2} \text{ again!}$$

2. Which of the following is a field? If it is a finite field, how many elements does it have?

(a)  $\mathbb{Z}[x]/\langle x^2 + x + 1 \rangle$ .

Not a field, eg 2 will not have an inverse  
( $\mathbb{Z}$  is not a field!)

(b)  $\mathbb{Q}[x]/\langle x^2 + x + 3 \rangle$ .

A field as  $x^2 + x + 3$  is irreducible in  $\mathbb{Q}[x]$   
(no roots)

(c)  $\mathbb{Z}_5[x]/\langle x^2 + x + 1 \rangle$ .

A field as  $x^2 + x + 1$  is irreducible in  $\mathbb{Z}_5[x]$   
(no roots)

$$\text{Size} = \underline{25}$$

(d)  $\mathbb{Z}_5[x]/\langle x^2 + x + 3 \rangle$ .

Not a field -  $x=1$  is a root of  $x^2 + x + 3$   
 $x=3$  is a root

$$\mathbb{Z}_5[x]/\langle x^2 + x + 3 \rangle = \mathbb{Z}_5[x]/\langle (x-1)(x-3) \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$$

CRT

2 which is not a field.

3. Let  $R$  be a principal ideal domain (definition?). Let  $a, b \in R$  be non-zero elements. Prove that a greatest common divisor of  $a$  and  $b$  (definition?) always exists. Show moreover that it can be expressed as a linear combination of  $a$  and  $b$ .

Consider  $I = \langle a, b \rangle$ .

It's principal, so equals  $\langle d \rangle$  some  $d \in R$ .

Note  $d \in \langle a, b \rangle$ , so  $d = sa + tb$  for  $s, t \in R$ .

(That's the moreover).

Claim  $d = \text{GCD}(a, b)$ .

Well  $a \in \langle d \rangle \therefore d \mid a$

Similarly,  $d \mid b$

Now say  $c \mid a$  and  $c \mid b$ .

Then  $c \mid sa + tb \therefore c \mid d$

}

}

these are the

defining properties  
of  $\text{GCD}(a, b)$

4. (a) Explain carefully why the polynomial  $x^3 + 5x + 2$  is irreducible in  $\mathbb{Z}_7[x]$ .

No roots  $\therefore$  No linear factors  
in  $\mathbb{Z}_7$

As its a cubic this proves  
its irreducible.

(b) Write down a basis for  $\mathbb{Z}_7[x]/\langle x^3 + 5x + 2 \rangle$  as a  $\mathbb{Z}_7$ -vector space. What is  $[\mathbb{Z}_7[x]/\langle x^3 + 5x + 2 \rangle : \mathbb{Z}_7]$ ?

$1, x, x^2$

Degree = 3

(c) Let  $F = \mathbb{Z}_7[x]/\langle x^3 + 5x + 2 \rangle$ . Let  $u = x + \langle x^3 + 5x + 2 \rangle$ . Express each of the three roots of the polynomial  $x^3 + 5x + 2$  in the form  $a + bu + cu^2$  for  $a, b, c \in \mathbb{Z}_7$ .

One is  $\boxed{u}$  of course.

Another will be  $u^7$

(a)  $p \mapsto p^7$  is an automorphism  
fixing element of  $\mathbb{Z}_7$

$$= u(2u+5)^2 = u(4u^2 + 6u + 4)$$

$$= 4(2u+5) + 6u^2 + 4u = \boxed{6u^2 + 5u + 6}$$

Another will be  $6(6u^2 + 5u + 6)^2 + 5(6u^2 + 5u + 6) + 6$

$$= 6(u^2 + 2u + 1)^2 - 5(u^2 + 2u + 1) + 6$$

$$= 6(u^4 + 4u^2 + 1 + 4u^3 + 4u + 2u^2) + 2u^2 + 4u + 1$$

$$= 6(2u^2 + 5u + u + 6 - u^2 + 4u + 1) + 2u^2 + 4u + 1$$

$$= -u^2 - 3u + 2u^2 + 4u + 1$$

$$= \boxed{u^2 + u + 1}$$

I hope  
I got  
the algebra  
right!

5. (a) What is an isomorphism  $f: R \rightarrow S$  between two rings?

Homomorphism - additive, multiplicative,  $f(1) = 1$   
 +  
Bijection.

(b) By considering a suitable evaluation homomorphism, prove that  $\mathbb{Q}[x]/\langle x^2 - 5 \rangle$  is isomorphic to  $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ .

$$\text{ev}_{\sqrt{5}}: \mathbb{Q}[x] \longrightarrow \mathbb{R}$$

$$\text{Image is } \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$$

kernel is  $\langle m_{\sqrt{5}}(x) \rangle$  where  $m_{\sqrt{5}}(x)$  is monic poly in  $\mathbb{Q}[x]$  of smallest degree that has  $\sqrt{5}$  as a root

$$\text{That: } \langle x^2 - 5 \rangle$$

$$\therefore \text{1st} \cong \text{2nd} \Rightarrow \mathbb{Q}[x] / \langle x^2 - 5 \rangle \cong \mathbb{Q}[\sqrt{5}]$$

↑  
a field

↑  
∴ a field

∴ Equals  $\mathbb{Q}(\sqrt{5})$ .

(c) Is  $\mathbb{R}[x]/\langle x^2 - 5 \rangle$  isomorphic to  $\mathbb{R}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{R}\}$ ?

No, it's  $\mathbb{R} \times \mathbb{R}$  by CRT. This is just  $\mathbb{R}$ .

6. Let  $E \subseteq F$  be a finite field extension such that  $[F : E]$  is prime. Suppose that  $u \in F$  is algebraic over  $E$ .

(a) What are the possibilities for the degree of  $u$  over  $E$ ?

$$1 \text{ or } [F : E]$$

(a)  $[E(u) : E]$  divides  $[F : E]$  by the tower law and  $[F : E]$  is prime)

(b) Suppose that  $a$  and  $b$  are complex numbers such that  $[\mathbb{Q}(a) : \mathbb{Q}] = 5$  and  $[\mathbb{Q}(b) : \mathbb{Q}] = 7$ . Calculate  $[\mathbb{Q}(a, b) : \mathbb{Q}]$ .

$$\begin{array}{c} \mathbb{Q} \subset \mathbb{Q}(a) \\ \mathbb{Q} \subset \mathbb{Q}(b) \end{array} \subset \mathbb{Q}(a, b)$$

Know: its  $\leq 35$ ,  
divisible by 5 and 7

$\therefore$  its  $\boxed{35}$  exactly

(c) For  $a$  and  $b$  as in (b), write down a basis for  $\mathbb{Q}(a, b)$  as a  $\mathbb{Q}$ -vector space.

$$\{ a^i b^j \mid 0 \leq i \leq 4, 0 \leq j \leq 6 \}$$

7. Check you know the following definitions:

(a) Subfield.

(b) The minimal polynomial of an algebraic element  $u \in F$  over a subfield  $E$ . (Explain *why* there is a unique such thing.)

$$\begin{aligned} & \text{ev}_u: F[x] \rightarrow E, f(x) \mapsto f(u) \\ \text{Ker ev}_u &= \langle m_u(x) \rangle \quad \text{as } F[x] \text{ is a PID} \\ & \quad \swarrow \text{monic, unique.} \end{aligned}$$

(c) The field of fractions of an integral domain  $R$ . What do elements of the field of fractions of  $F[x]$  look like? (This is usually denoted  $F(x)$ .)

$$\text{rational fractions } \frac{f(x)}{g(x)} \text{ with } g(x) \neq 0.$$

(d) Unique factorization domain.

8. Take a look back at the two midterms this term! Solutions to them both are posted on the web!