Exam 1

Modern Algebra II, Dave Bayer, October 2, 2008

Name: Answers

[1] (6 pts)	[2] (6 pts)	[3] (6 pts)	[4] (6 pts)	[5] (6 pts)	TOTAL

Please work only one problem per page, starting with the pages provided. Clearly label your answer. If a problem continues on a new page, clearly state this fact on both the old and the new pages.

[1] Define a ring homomorphism. Define an ideal. Prove that the kernel of a ring homomorphism is an ideal.

$f: R \to S$ is a ring homomorphism $\iff$
one can add, multiply before or after applying f

$I \subset R$ is an ideal $\iff$
I is an additive subgroup of $(R,+)$,
and I "acts like 0" multiplicatively:
for any $a \in R$, $b \in I$, $ab \in I$ and $ba \in I$
$(a \in R,\ 0,\ a0 = 0 \quad 0a = 0)$

$\ker(f) = \{a \in R \mid f(a) = 0\}$

closed under $+$: $a, b \in \ker(f)$
$\Rightarrow f(a) = 0,\ f(b) = 0$
$\Rightarrow f(a+b) = f(a) + f(b) = 0+0 = 0$
$\Rightarrow a+b \in \ker(f)$

closed under $*$: $a \in R,\ b \in \ker(f)$
$\Rightarrow f(ab) = f(a)f(b) = f(a)0 = 0$
(check also ba) ✓ $\Rightarrow ab \in \ker(f)$

[2] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)^3 = 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

$$e^{xt} = e^{[2+(x-2)]t} = e^{2t}e^{(x-2)t}$$

working in $\mathbb{R}[x]/((x-2)^3)$,

$$e^{(x-t)t} = 1 + (x-2)t + \tfrac{1}{2}(x-2)^2t^2$$

$$\Rightarrow \quad e^{At} = e^{2t}\left[I + (A-2I)t + \tfrac{1}{2}(A-2I)^2t^2\right]$$

example: $$A = \begin{bmatrix} 2 & 1 & \\ & 2 & 1 \\ & & 2 \end{bmatrix}$$

$$e^{At} = e^{2t}\left[\begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{bmatrix}t + \frac{1}{2}\begin{bmatrix} 0 & 0 & 1 \\ & 0 & 0 \\ & & 0 \end{bmatrix}t^2\right]$$

$$= e^{2t}\begin{bmatrix} 1 & t & \frac{1}{2}t^2 \\ & 1 & t \\ & & 1 \end{bmatrix} \quad \checkmark$$

[3] Construct the finite field $\mathbb{F}_8$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_2$. What are the three roots of your irreducible polynomial?

$x^3 + ax^2 + bx + c$

x^3	a	b	c	0?	1?
1	1	1	1		✓
1	1	1	0	✓	
1	1	0	1		
1	1	0	0	✓	✓
1	0	1	1		
1	0	1	0	✓	✓
1	0	0	1		✓
1	0	0	0	✓	

irreducible, or has root.

irreducible,

$x^3 + x^2 + 1$

$\boxed{x^3 + x + 1}$

use this

(or use the first one!)

$$\boxed{\mathbb{F}_8 = \mathbb{F}_2[x] / (x^3+x+1)}$$

$\Rightarrow$ x is a root of $z^3 + z + 1$, by design.

$x^2,\ x^4 = xx^3 = x(x+1) = x^2+x$ are other roots:

$$(z+x)(z+x^2)(z+(x^2+x))$$

$$= z^3 + \underbrace{(x + x^2 + (x^2+x))}_{0} z^2 + (x\cdot x^2 + x(x^2+x) + x^2(x^2+x))\, z + (x \cdot x^2 \cdot (x^2+x))$$

$$x \cdot x^2 + (x^2+x)^2 = x+1 + x^8 = x+1+x \quad (x^8 = x!) = 1 \quad ✓$$

$$x^3 \cdot (x^2+x) = x^3 \cdot x^3 \cdot x = x^7 = 1 \quad ✓$$

$$\boxed{\text{roots of } z^3+z+1 = 0 \text{ are } x,\ x^2,\ x^2+x}$$

[4] A message is represented as an integer a mod 35. You receive the encrypted message $a^5 \equiv 3 \mod 35$. What is a?

$$\mathbb{Z}/35\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

$\mathbb{Z}/5\mathbb{Z}$ multiplicative group has order 4, so $x^4 = 1$

$\Rightarrow$ for any x in $\mathbb{Z}/5\mathbb{Z}$, $x^5 = x$

for any m more generally, $x^{4m+1} = x$

$\mathbb{Z}/7\mathbb{Z}$ $\Rightarrow$ for any m, $x^{6m+1} = x$

To be 1 mod 4 and 1 mod 6, be 1 mod lcm(4,6)

1 mod 12.

Want to find decoding exponent e so $(a^5)^e = a$

By above, want e so $5e \equiv 1 \mod 12$

$5 \cdot 5 = 25 \equiv 1 \mod 12$

$\Rightarrow$ $3^5 = 3^4 \cdot 3 = 81 \cdot 3 \equiv 11 \cdot 3 = 33 \mod 35$

$\boxed{\text{message was "33"}}$

check $33^5 \equiv (-2)^5 = -32 \equiv 3 \mod 35$ ✓

[5] Give an example of a finite ring R which is not a field, such that $1 \neq 0$ but $1 + 1 + 1 = 0$.

$$\mathbb{Z}/3\mathbb{Z}[x]/(x^2) \qquad (\text{so } x \cdot x = 0)$$

---

or find two quadratic irred polys, take product

$x^2 + ax + b$			0?	1?	2?	irred	
1	0	0	✓				
1	0	1				*	x^2+1
1	0	2		✓	✓		
1	1	0	✓		✓		
1	1	1		✓			
1	1	2				*	x^2+x+2
1	2	0	✓	✓			
1	2	1			✓		
1	2	2				*	x^2+2x+2

$$\mathbb{Z}/3\mathbb{Z}[x]/((x^2+1)(x^2+x+2))$$

(so $(x^2+1)\cdot(x^2+x+2) = 0$, not a field.)