ALGEBRAIC SYSTEMS
Final Exam
December 17, 2009

The point value of each problem is given in the margin. Total = 160 points.

(12) 1. Use the Euclidean Algorithm to find the greatest common divisor \( d \) of 105 and 147 and find integers \( x, y \) such that \( 147x + 105y = d \).

\[
\begin{array}{cccc}
147 & 105 & 42 & 21 \\
147 & 105 & 42 & 21 \\
0 & 2 & 3 & 0 \\
\end{array}
\]

There are actually 3 among solutions

\[
\begin{align*}
\gcd(105, 147) &= \gcd(105, 42) \\
&= \gcd(21, 42) \\
&= \gcd(21, 0) \\
&= 21
\end{align*}
\]

and \( 147(-2) + 105(3) = 21 \)

(12) 2. Prove by induction that for any positive integer \( n \), \( \sum_{k=1}^{n} (2k-1) = n^2 \).

Base case: For \( n = 1 \) we have \( \sum_{k=1}^{1} (2k-1) = 2 \cdot 1 - 1 = 1 \), so True.

Assume the statement is true for \( n \), that is \( \sum_{k=1}^{n} (2k-1) = n^2 \), *Assume *

and consider \( n+1 *\)

\[
\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^{n} (2k-1) + (2(n+1)-1)
\]

\[
= n^2 + (2(n+1)-1), \text{ by induction } \text{Assume } *
\]

\[
= n^2 + 2n + 1
\]

\[
= (n+1)^2 \quad \text{Q.E.D.}
\]
3. Calculate the following values using properties of congruences.

a) \( 602^3 \cdot 59 \mod 6 \)
\[
\equiv 2^3 \cdot (-1) \equiv -8 \equiv -2 \equiv 4 \mod 6
\]

b) \((14)^{162} \mod 17\) (You can use Fermat's Little Theorem.)
\[
\text{Since } 17 \nmid 14, \text{ by FLT } 14^{16} \equiv 1 \mod 17
\]
\[
\Rightarrow 14^{16^2} \equiv 14^{16 \cdot 10 + 2} \equiv (14^{16})^{10} \cdot 14^2 \mod 17
\]
\[
\equiv 1^{10} \cdot (-3)^2 \equiv 9 \mod 17.
\]

c) \(5^{-1} \mod 7\)
By trial and error, \(5 \cdot 3 = 15 \equiv 1 \mod 7\)
Thus \(5^{-1} \equiv 3 \mod 7\)
(or solve eqn \(5x + 7y = 1\) to get \(x \equiv 5^{-1} \mod 7\))

4. Prove that if \(d|a\) and \(d|b\) then \(d|(a+b)\).

Suppose that \(d|a\) and \(d|b\). Then \(a = dk\) and \(b = dl\) for some integers \(k, l\). Thus \(a+b = dk + dl = d(k+l)\). Since \(k + l \in \mathbb{Z}\), we conclude that \(d|(a+b)\).
5. Let \( z = \sqrt{3} + i \in \mathbb{C} \).

(4) a) Express \( z \) in polar form.

\[
|z| = \sqrt{(\sqrt{3})^2 + 1^2} = \sqrt{4} = 2
\]

\[
z = r \ e^{i \theta} = 2 \ e^{i \pi/6}
\]

or \( 2 (\cos(\pi/6) + i \sin(\pi/6)) \).

(4) b) Find \( z^{18} \). Express your answer in standard form \( a + bi \).

\[
z^{18} = (2 \ e^{i \pi/6})^{18} = 2^{18} \ e^{i \ 3\pi} = 2^{18} \ e^{i \pi} = 2^{18} (-1) = -2^{18}
\]

(8) 6. Factor the polynomial \( x^4 + 1 \) completely over \( \mathbb{C} \).

First find zeros: \( x^4 = -1 \) \( \Rightarrow \ x = (-1)^{1/4} = \left( e^{i \pi + 2i \pi k} \right)^{1/4} \)

\[
e^{i \pi/4} = e^{i \pi/4 + \pi/2 k}, \quad k = 0, 1, 2, 3
\]

\[
x^4 + 1 = (x - (\frac{1}{2} + \frac{1}{2} i))(x - (\frac{1}{2} - \frac{1}{2} i))(x - (\frac{1}{2} - \frac{1}{2} i))(x - (\frac{1}{2} + \frac{1}{2} i))
\]

(12) 7. a) List the elements of \( U_9 \), the group of units \( \mod 9 \).

\[
U_9 = \{ 1, 2, 4, 5, 7, 8 \}, \quad \text{All elements rel. prime to 9.}
\]

b) Give an example of a unit in the matrix ring \( M_{2,2}(\mathbb{Z}) \), other than the identity matrix, and show why it is a unit.

\[
\begin{bmatrix}
-1 & 0 \\
0 & 1
\end{bmatrix}
is a unit since
\begin{bmatrix}
-1 & 0 \\
0 & 1
\end{bmatrix}\begin{bmatrix}
-1 & 0 \\
0 & 1
\end{bmatrix} = \begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}
\]

c) Give an example of a zero divisor in \( M_{2,2}(\mathbb{Z}) \), and show why it is a zero divisor.

\[
\begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}\begin{bmatrix}
1 & 0 \\
0 & 0
\end{bmatrix} = \begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix}
The \begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix} and \begin{bmatrix}
1 & 0 \\
0 & 0
\end{bmatrix} are zero divisors.
\]

d) Find \( |M_{2,2}(\mathbb{Z}_3)| = 3^4 \), since there are 3 choices for each entry.
8. Indicate whether the following sets are closed under addition (C.A.), closed under multiplication (C.M.), Additive Groups (A.Group), Rings (Ring), Integral Domains (Domain), Fields (Field). Circle all correct answers on each problem.

a) \( \mathbb{Z}_{16} \)  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ \neg \exists \, 3 \cdot 5 = 0 \]

b) \( \mathbb{R}^* = \mathbb{R} - \{0\} \)  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ 1 + (-1) = 0 \notin \mathbb{R}^* \]

c) \( \mathbb{E}[x] \), the set of polynomials all of whose coefficients are even integers (\( \mathbb{E} = \{2n : n \in \mathbb{Z}\} \)).  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ \neg \text{No identity } 1 \]

d) \( \{a + bi : a, b \in \mathbb{Q}\} \) (\( i = \sqrt{-1} \))  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ \text{Note: } \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a^2}{a^2+b^2} - \frac{b^2}{a^2+b^2} i \in \mathbb{S}, \text{ since } \frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Q} \]

e) \( \{a + bx : a, b \in \mathbb{Z}_2\} \)  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ \neg \text{no, linear - linear = quadratic } \notin \mathbb{S} \]

f) \( 1^{1/7} = \{e^{2\pi ki/17} : k = 0, 1, 2, \ldots, 16\} \)  
\[ \text{C.A. C.M. A.Group Ring Domain Field} \]
\[ \{ \in \mathbb{S}, \text{ but } 1 + 1 \notin \mathbb{S} \]

9. State and prove the conjugate zero theorem for polynomials over \( \mathbb{R} \).

\[ \text{Thm Let } f(x) \text{ be a polynomial over } \mathbb{R}, f(x) = a_n x^n + \cdots + a_0, \text{ with complex zero } z. \text{ Then } \overline{z} \text{ is also a zero of } f(x). \]

\[ \text{Prf. Suppose } z \text{ is a zero of } f(x), \text{ Then } \]
\[ f(z) = 0 \]
\[ \implies a_n z^n + \cdots + a_0 = 0 \]
\[ \implies \frac{a_n z^n + \cdots + a_0}{a_n} = 0 \]
\[ \implies a_n \overline{z}^n + \cdots + \overline{a}_0 = 0 \]
\[ \implies a_n \overline{z}^n + \cdots + \overline{a}_0 = 0 \]

Here we have used the properties \( \overline{z + \overline{v}} = z + \overline{v} \) and \( \overline{z \cdot \overline{v}} = \overline{z} \cdot \overline{v} \).
10. Prove the following part of the factor theorem for polynomials \( f(x) \) over a field \( F \).

If \( r \) is a root (zero) of \( f(x) \) then \( (x-r) \) is a factor of \( f(x) \).

\[ L.F. \quad \text{By the division algorithm,} \quad f(x) = g(x)(x-r) + r(x), \]

for some \( g(x), r(x) \in F[x] \) with either \( r(x) = 0 \) or \( \deg r(x) < 1 \).

In either case \( r(x) \) is a constant, say \( r(x) = R \), with \( R \in F \).

Thus \( f(x) = g(x)(x-r) + R \). *

Inserting \( x = r \), we get \( f(r) = g(r)(r-r) + R = R \), but since \( r \) is a zero of \( f(x) \), \( f(r) = 0 \). Therefore \( R = 0 \) and so by *, \( f(x) = g(x)(x-r) \), that is, \( (x-r) \) is a factor of \( f(x) \).

11. Let \( \alpha \in S_7 \) be the permutation

\[ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 7 & 5 & 2 & 4 \end{pmatrix}, \]

a) Express \( \alpha \) as a product of disjoint cycles.

\[ \alpha = (1, 3)(2, 6)(4, 7) \]

b) Find \( \alpha^{-1} \) (in standard form or cycle form).

\[ \alpha^{-1} = \alpha = (1, 3)(2, 6)(4, 7) \]

c) Let \( \beta = (1, 2, 7) \). Find \( \beta^2 \alpha \) (in standard form or cycle form).

\[ \beta^2 = (1, 3, 7)(1, 3, 7) = (1, 7, 2). \quad \text{Thus} \]

\[ \beta^2 \alpha = (1, 7, 2)(1, 3)(2, 6)(4, 7) \]

\[ = (1, 3, 7, 1, 2, 6) \]

\(< \text{Note, this denotes function comp. so you go right to left. Thus} \>

\[ 1 \to 3 \text{ step} \]

\[ 3 \to 1 \to 7 \]

\[ 7 \to 4 \]

\[ 4 \to 7 \to 2 \]

\[ 2 \to 6 \]

\[ 6 \to 2 \to 1 \]
12. a) Is \((\mathbb{Z}_4, +)\) a cyclic group? Explain. Yes \(\mathbb{Z}_4 = \langle 1 \rangle\)

b) Give an example of a nonabelian group. \(S_n = n\text{-th symmetric group}
\text{for } n \geq 3\)
\((\text{Also } D_n, \text{ for } n \geq 3)\).

c) Give an example of an infinite group.
\[
\left( \mathbb{H}, + \right) \subset \left( \mathbb{R}^*, \cdot \right), \text{ etc.}
\]

d) What is the order of the symmetric group \(S_4\)? \(|S_4| = 4! = 24\)

13. Let \(D_6 = \langle \sigma, \tau \rangle\) be the dihedral group of symmetries of a regular hexagon, with \(\sigma = (1, 2, 3, 4, 5, 6)\) being rotation clockwise 60° and \(\tau = (2, 6)(3, 5)\) being a flip about the axis through 1 and 4.

a) Find \(\sigma \tau\) (in cycle notation).
\[
\sigma \tau = (1, 2, 3, 4, 5, 6)(2, 6)(3, 5) = (1, 2)(3, 6)(4, 5)
\]

b) What symmetry of the hexagon is \(\sigma \tau\)? A flip about the vertical axis bisecting segments \(\overline{12}\) and \(\overline{54}\).

c) Determine \(\text{ord}(\sigma) = 6\) and \(\text{ord}(\tau) = 2\)
\[
\tau^2 = 1, \quad \sigma^2 = \sigma, \quad \tau^2 = \tau
\]

d) Give the order of \(D_6\): \(|D_6| = 2 \cdot 6 = 12\)

14. a) What is the largest order of any element of the dihedral group \(D_8\)? Explain. 8

Let \(\tau\) be rotation \(\frac{2\pi}{8}\) clockwise. Clearly \(\text{ord}(\tau) = 8\) and \(\text{ord}(\sigma^i)\) for any \(i \in \mathbb{N}\). The other symmetries are flips, each of order 2.

b) What is the largest order of any element of the symmetric group \(S_8\)? Explain. Let \(x \in S_8\).

We consider all possible decompositions of \(x\) as a product of disjoint cycles.

i) \(x = (8\text{-cycle})\), \(\text{ord}(x) = 8\)

ii) \(x = (7\text{-cycle}), (1\text{-cycle})\), \(\text{ord}(x) = 7\)

iii) \(x = (6\text{-cycle}), (2\text{-cycle})\), \(\text{ord}(x) = 6\)

iv) \(x = (5\text{-cycle}), (3\text{-cycle})\), \(\text{ord}(x) = 15\)

v) \(x = (5\text{-cycle}), (2\text{-cycle})(1\text{cycle})\), \(\text{ord}(x) = 10\)

vi) \(x = (4\text{-cycle})(3\text{-cycle})(1\text{cycle})\), \(\text{ord}(x) = 12\)

vii) \(x = (4\text{-cycle})(2\text{-cycle})(2\text{cycle})\), \(\text{ord}(x) = 4\)

\(\vdots\) etc. All others, \(\text{ord} \leq 6\).

Clearly, the largest order is 15.