ALGEBRAIC SYSTEMS

Exam 3
December 1, 2006

The point value of each problem is given in the margin. Total = 80 points.

(10)  1) Indicate whether the given polynomial is reducible or irreducible over the given ring. Circle the correct answer. No work needs to be shown.
   a) \(5x^2 - 15\) over \(\mathbb{Q}\). reducible irreducible
      \[5(x^2 - 3), \text{ since } 5 \text{ is a unit in } \mathbb{Q} \text{ and } x^2 - 3 \text{ has no rational zero}
      \text{ the poly. is irreducible over } \mathbb{Q}\]
   b) \(x^4 + 1\) over \(\mathbb{Z}_2\). reducible irreducible
      \(2x^2 + 1 = 0\) for \(x = 1, 1 = 0\), thus \((x - 1)\) is a factor
   c) \(x^6 + x^3 - 3x + 17\) over \(\mathbb{C}\). reducible irreducible
      All poly's over \(\mathbb{C}\) factor into linear factors.
   d) \(x^3 + x + 17\) over \(\mathbb{Q}\). reducible irreducible
      By rational root test, \(\pm 1, \pm 17\) are the only possible roots, but none of them works. Thus there
      is no linear factor.
   e) \(x^3 + x + 17\) over \(\mathbb{R}\). reducible irreducible
      Only linear poly's and quadratics with neg. discriminants are irreducible over \(\mathbb{R}\).

(8)  2. State and prove the factor theorem for polynomials over a field \(F\). (Use the division algorithm for your proof. Do not assume the remainder theorem.)

Let \(f(x) \in F[x], a \in F\). Then \(a\) is a zero of \(f(x)\) if and only if \((x-a)\) is a factor of \(f(x)\).

Proof. By the division algorithm \(f(x) = q(x)(x-a) + r(x)\) for some polynomials \(q(x), r(x)\) with \(\deg(r(x)) < 1\) or \(r(x) = 0\).
In either case \(r(x)\) is a constant polynomial, say \(r(x) = r \in F\).
Thus \(f(x) = q(x)(x-a) + r\).

Then \(a\) is a zero of \(f(x)\):

\[\Leftrightarrow f(a) = 0\]
\[\Leftrightarrow q(a)(a-a) + r = 0\]
\[\Leftrightarrow r = 0\]
\[\Leftrightarrow f(x) = q(x)(x-a), \text{ for some } q(x) \in F[x]\]
\[\Leftrightarrow (x-a) \text{ is a factor of } f(x)\].
3) a) Define what it means for a set \( G \) with binary operation \( * \) to be a group.

\[ G, * \] is a group if

i) \( G \) is closed under \( * \), that is, if \( x, y \in G \), then \( x*y \in G \)

ii) \( * \) is associative, that is, \( (x*y)*z = x*(y*z) \) \( \forall x, y, z \in G \)

iii) \( G \) has an identity \( e \) satisfying \( x*e = e*x = x \), \( \forall x \in G \)

iv) For any \( x \in G \), there is an inverse \( x' \) in \( G \) such that \( x*x' = e \), \( x'*x = e \)

b) Give an example of a nonabelian group.

\[ S_n, (\text{for any } n \geq 3) \], \( D_n, (\text{for any } n \geq 3) \)

c) Give examples of two different groups of order 8.

\[ \{ \mathbb{Z}_8, + \}, D_4 \]

4. Determine whether the following sets are groups under the given operation. If not, state one property that fails.

a) \( \{ \pm 1, \pm i \} \) under multiplication. (Here, \( i = \sqrt{-1} \).) \[ \text{Group} \]

b) The set of multiples of 3, \( \{ 3x : x \in \mathbb{Z} \} \), under addition. \[ \text{Group} \]

c) The set of units modulo 9, \( U_9 \), under addition. \[ U_9 = \{1, 2, 4, 5, 7, 8\} \]

\[ \text{Not closed under +; } 1 + 2 = 3 \notin U_9 \]

\[ \text{Not a group} \]

d) The set of nonzero complex numbers under multiplication. \[ \text{Group} \]

5) Let \( U_7 \) be the multiplicative group of units \( (\text{mod } 7) \).

a) What is the order of \( U_7 \)? \[ |U_7| = \phi(7) = 6 \]

b) Find an element in \( U_7 \) of order 3.

\[ 2^3 \equiv 1 \pmod{7} \]

\[ \text{But } 2^4 \equiv 2 \pmod{7} \]

\[ \text{Thus the order of } 2 \text{ is 3.} \]

c) Find a subgroup of \( U_7 \) of order 3.

\[ < 2 > = \{ 1, 2, 4 \} \]

\[ \{ \mathbb{Z}_8, + \}, D_4 \]
(9) 6) Let \( \mathbb{Z}_8 \) be the additive group of residue classes \( \text{mod } 8 \).
   a) Is \( \mathbb{Z}_8 \) a cyclic group? If so, give a generator for the group.
   \[ \text{Yes, } \mathbb{Z}_8 = \langle [1] \rangle \]

b) What is the order of 2?
   \[ 2 + 2 + 2 = 4, \quad 2 + 2 + 2 + 2 = 8 = 0 \]
   Thus the order of 2 is 4.

c) What is the inverse of 3 with respect to the group operation.
   \[ -3 = 5 \quad \text{since} \quad 5 + 3 = 0 \quad \text{in } \mathbb{Z}_8. \]

(9) 7) Let \( \alpha \in S_7 \) be the permutation
   \[ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 5 & 4 & 7 & 2 \end{pmatrix} \]

a) Express \( \alpha \) as a product of disjoint cycles.
   \[ \alpha = (1, 3)(2, 6, 7)(4, 5) \]

b) Find \( \alpha^{-1} \), expressed in both standard form and as a product of cycles. (Standard form means the way \( \alpha \) is defined above.)
   \[ \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 1 & 5 & 4 & 2 & 6 \end{pmatrix} \]
   \[ \alpha^{-1} = (1, 3)(2, 7, 6)(4, 5) \]

c) Find \( \alpha^2 \). (Expressed in standard form or cycle form.)
   1) Standard Form: \( \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 4 & 5 & 2 & 6 \end{pmatrix} \)
   \[ \alpha^2 = (1, 3)(2, 6, 7)(4, 5)(1, 3)(2, 6, 7)(4, 5) = (1)(2, 7, 6)(4)(5) = (2, 7, 6) \]
   2) A second way:
      \[ \alpha^2 = (1, 3)(2, 6, 7)(4, 5)^2 = (2, 6, 7)^2 = (2, 7, 6) \]
(8) b) Let \( \sigma, \tau \) be symmetries of a square corresponding to clockwise rotation of 90 degrees and a flip around the vertical axis resp., \( \sigma = (1,2,3,4), \tau = (1,2)(3,4) \).

\[ \begin{align*}
\sigma \tau &= (1,2,3,4)(1,2)(3,4) = (1,3)(2,4) = (1,4) \\
\tau \sigma &= (1,2)(3,4)(1,2,3,4) = (1)(2,4)(3) = (2,4)
\end{align*} \]

a) Find \( \sigma \tau \) and \( \tau \sigma \) expressed in cycle notation. (Recall, \( \sigma \tau \) means apply \( \tau \) first, then \( \sigma \).)

\[ \begin{align*}
\sigma \tau &= (1,3) \text{, a flip about } D_2 \\
\tau \sigma &= (2,4) \text{, a flip about } D_1
\end{align*} \]

b) State in words the symmetries of the square corresponding to \( \sigma \tau \) and \( \tau \sigma \).

(4) 8) a) State the Fundamental Theorem of Algebra. Let \( f(x) \) be a nonconstant polynomial with complex coefficients. Then \( f(x) \) has a zero in \( \mathbb{C} \).

(8) b) State and prove the linear factorization theorem for polynomials over \( \mathbb{C} \). (Use induction.)

If \( f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x] \), then there exist complex numbers \( r_1, r_2, \ldots, r_n \) such that \( f(x) = a_n (x-r_1)(x-r_2) \cdots (x-r_n) \).

**Proof.** By induction on \( n \). When \( n = 1 \), \( f(x) = a_1 x + a_0 \) with \( a_0 \neq 0 \). Then \( f(x) = a_1 (x + \frac{a_0}{a_1}) = a_1 (x - r_1) \) with \( r_1 = -\frac{a_0}{a_1} \in \mathbb{C} \).

Suppose the statement is true for \( n \) and let \( f(x) \) be of degree \( n+1 \). By Fund. Thm. of Algebra \( f(x) \) has a zero \( r \in \mathbb{C} \) and so by the factor theorem \( f(x) = (x-r) g(x) \) for some polynomial \( g(x) \) over \( \mathbb{C} \). Now \( g(x) \) has degree \( n \) and has the same leading coeff. as \( f(x) \), call it \( a_n \). Thus, by induction assumption there exist complex numbers \( r_1, \ldots, r_n \) such that \( g(x) = a_n (x-r_1) \cdots (x-r_n) \). Then \( f(x) = a_n (x-r) (x-r_1) \cdots (x-r_n) \) Q.E.D.