

Math 558 Spring 2009

Review for second exam

I. Calculations

1. Find the remainder in $\mathbb{Z}_7[x]$ when you divide $x^{143} + 3x$ by $x + 6$. [Hint: don't even think of dividing.]

Answer. $6 \equiv -1 \pmod{7}$, so we're dividing by $x - 1$. Hence the remainder is $1^{143} + 3(1) = 4$.

2. Factor $x^4 + 1$ completely in \mathbb{Z}_2 .

Answer. $(x + 1)^4$.

3. Using the Euclidean algorithm, find a gcd of $x^4 + x^2 + 3$ and $x^6 + 4x^4 + x^2 + 4$ in (a) \mathbb{R} ; (b) $\mathbb{Z}_5[x]$.

Answer. (a) they are relative prime, i.e., 1 is a gcd. (b) $x^4 + x^2 + 3$.

4. If $x^3 + ax^2 + bx + c$ has roots $r, -r, r^2$, what are a, b, c ?

Answer. $a = -r^2; b = -r^2; c = r^4$.

5. If $\deg P = 8$ and P has roots (counting multiplicities) $r, r, s, s, -r, -r, -s, -s$, what is the coefficient of x^7 ? Of x^6 ? What is the constant term?

Answer. Coefficient of $x^7 = 0$. Coefficient of $x^6 = 0$. Constant term $= r^4 s^4$.

6. (a) Show that $x^3 + x + 4$ is irreducible in \mathbb{Z}_{11} .

Answer. It has no zeroes and has degree 3. (I used a calculator to show that it had no zeroes.)

(b) If γ is a Galois imaginary for $x^3 + x + 4$ over \mathbb{Z}_{11} , what's γ^5 ?

Answer. $\gamma^3 = -\gamma - 4 = 10\gamma + 7$, so $\gamma^4 = 10\gamma^2 + 7\gamma$, and $\gamma^5 = 10\gamma^3 + 7\gamma^2 = 10(10\gamma + 7) + 7\gamma^2 = 100\gamma + 70 + 7\gamma^2 = \gamma + 7\gamma^2 + 4$.

7. For each of the following functions, say whether it is invariant. If it is not invariant, say how many variants it has:

(a) $rst + stu$

Answer. Not invariant. Has $\binom{4}{2} = 6$ variants.

(b) $\frac{rst}{r+s+t+u}$

Answer. Not invariant. Has $\binom{4}{3} = 4$ variants.

(c) $rs + rst + rstu$

Answer. Not invariant. Has $\binom{4}{2} \cdot \binom{2}{1} = 12$ variants.

8. Let $f = x_1x_2 + x_3x_4 + x_5x_6$.

(a) if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 1 & 2 \end{pmatrix}$, what's σf ?

Answer. $x_4x_3 + x_5x_6 + x_1x_2$

(b) If $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 1 & 2 & 4 \end{pmatrix}$, what's τf ?

Answer. $x_5x_3 + x_6x_1 + x_2x_4$.

(c) Are any of $f, \sigma f, \tau f$ equal?

Answer. $f = \sigma f$.

9. Which permutations leave $x_1x_2 + x_1x_3 + x_1x_4$ invariant?

Answer. Any σ with $\sigma(1) = 1$.

10. Write a function of three variables that has exactly two variants.

Answer. $(x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$.

11. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 10 & 6 & 7 & 4 & 8 \end{pmatrix}$

(a) Decompose σ into disjoint cycles.

Answer. $(1\ 5\ 3)(2\ 9\ 4)(6\ 10\ 8\ 7)$

(b) What's σ^{-1} ?

Answer. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 9 & 1 & 7 & 8 & 10 & 2 & 6 \end{pmatrix}$

12. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 10 & 6 & 7 & 4 & 8 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 8 & 2 & 9 & 7 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$.

What's $\sigma\tau$?

Answer. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 9 & 4 & 6 & 2 & 5 & 1 & 10 & 3 \end{pmatrix}$

13. Decompose (13542) as a composition of transpositions in two distinct ways.

Answer. $(12)(14)(15)(13)$; $(13)(35)(54)(42)$. [Other answers are possible.]

II. Short Answer

1. Yes or no:

(a) In $R[x]$ are there polynomials A, B so $(x^2 - 1)A + (x^4 - 1)B = 5x - 5$?

Answer. No. $x - 1$ is a common divisor, but not a gcd; $x^2 - 1$ is a gcd.

(b) In $R[x]$ are there polynomials A, B so $(x^2 - 1)A + (x^4 - 1)B = 5x^2 - 5$?

Answer. Yes, see (a).

2. Look at problem I.6. Why would it be really mean for me to ask you the order of γ ?

Answer. $\#GF^+ = 11^3 - 1 = 1330 = 266 \times 5$. If γ were primitive, you'd have to take its first 267th powers absolutely correctly to be sure.

3. Suppose $\deg P = 5$ and P is irreducible over \mathbb{Z}_7 .

(a) Is there an element α in $GF(7, P)$ with $o(\alpha) = 10$? Briefly explain.

Answer. No. $\#GF^+ = 16806$, which is not divisible by 10.

(b) Is there an element β in $GF(7, P)$ with $o(\beta) = 2801$? Briefly explain.

Answer. Yes, $2801 \times 6 = 16806$. More precisely, if γ is primitive, then $(\gamma^6) = 2801$.

4. Suppose for every $\alpha \in GF = GF(p, P)$ with $\alpha \neq 0, 1$, $o(\alpha) = 7$. What can you say about $\#GF^+$? About p ? About P ?

Answer. $\#GF^+ = 7$, so $p = 2$ and $\deg P = 3$.

6. Can a function of 20 variables have exactly 18 variants? Briefly explain.

Answer. Nope. Use Cauchy's theorem and note that $18 < 19 < 20$ and 19 is prime.

7. Which of the following is a group? Briefly explain.

(a) The set of even permutations in some $S!$

Answer. Yes. Check: Id is even; even \circ even is even; even⁻¹ is even.

(b) The set of odd permutations in some $S!$

Answer. No. Id is even. Also, no closure. [Just one of these suffices.]

(c) The set of permutations in S_7 that leave 3 fixed.

Answer. Yes. Check: $Id(3) = 3$; if $\sigma(3) = 3 = \tau(3)$ then $\sigma\tau(3) = 3$; $\sigma(3) = 3$ iff $\sigma^{-1}(3) = 3$.

(d) The set of permutations σ in S_7 for which $\sigma(2) = 5$.

Answer. No. $Id(2) \neq 5$. Also, no closure. And unless $\sigma(5) = 2, \sigma^{-1}(2) \neq 5$. [Just one of these suffices.]

(e) $\{1, 3, 5\}$ in (\mathbb{Z}_7, \cdot) .

Answer. Yes: odd \cdot odd is odd, 1 is the identity, and $3^{-1} = 5, 5^{-1} = 3$.

(f) $\{1, 3, 5\}$ in $(\mathbb{Z}_7, +)$.

Answer. No. No identity, no closure, no inverses. [Just one of these suffices.]

8. For which elements α of $GF(3, P)$ does $\alpha = -\alpha$?

Answer. Only 0. Why? In \mathbb{Z}_3 if $k + k = 0$ then $k = 0$. So in $GF(3, P)$, if $2\sum_{i \leq n} a_i x^i = 0$ then each $a_i = 0$.

III. Proofs and explanations

1. $x^4 + 1$ is irreducible in \mathbb{Z}_3 . Why?

Answer. We showed in class that in any field in which $x^4 + 1$ has no zeroes, if $x^4 + 1$ is reducible then $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$. In \mathbb{Z}_3 , $x^4 + 1$ has no zeroes. And in \mathbb{Z}_3 , 2 has no square root.

2. Let P be a linear polynomial which is not constant, and let Q be any polynomial. Prove there there are polynomials A, B so $AP + BQ = 1$ iff P, Q have no zeroes in common.

Answer. \Rightarrow : If there are A, B with $AP + BQ = 1$ then P, Q are relatively prime. If a were a common zero of P, Q , then P would have the form $c(x - a)$ and $x - a$ would be factor of Q , which contradicts P, Q relatively prime.

\Leftarrow : Since P is linear and not constant, it has a zero, a , and has the form $c(x - a)$. Since a is not a zero of Q , $x - a$ is not a factor of Q . So P, Q are relatively prime, and there are A, B with $AP + BQ = 1$.

3. (a) Prove that if p is a prime, $p > 2$, and P is irreducible over \mathbb{Z}_p , then the sum of the elements of $GF(p, P)$ equals 0.

Answer. Let $n = \deg P$. $x^{p^n} - x = \prod_{\alpha \in GF} (x - \alpha)$. $-\sum_{\alpha \in GF} \alpha$ is the coefficient of x^{p^n-1} in the Galois polynomial, which is 0.

(b) Prove that if p is a prime, $p > 2$, and P is irreducible over \mathbb{Z}_p , then the product of the elements of $GF(p, P)^+$ equals -1.

Answer. $\prod_{\alpha \in GF} (x - \alpha) = x^{p^n-1} - 1$, so $-1 = (-1)^{p^n-1} \prod_{\alpha \in GF} \alpha$. Since $p^n - 1$ is even, $-1 = \prod_{\alpha \in GF} \alpha$

(c) What happens for both sum and product in \mathbb{Z}_2 ?

Answer. For sum: $0 + 1 = 1$. For product: $1 = -1$.

(d) Prove that (b) holds if $p = 2$.

Answer. The same proof gives $-1 = (-1)^{p^n-1} \prod_{\alpha \in GF} \alpha$. But now $-1 = -\prod_{\alpha \in GF} \alpha$. So $\prod_{\alpha \in GF} \alpha = 1$. Which, in GF , is -1.

[Remark: Yes, (a) and (b) were homework problems. But this time I want a short and elegant proof.]

4. Show that if $\tau f = f$ for all transpositions τ then f is invariant.

Answer. Since every permutation σ is a composition of transpositions $\tau_1\tau_2\dots\tau_m$, $\sigma f = \tau_1\tau_2\dots\tau_{m-1}\tau_m f = \tau_1\tau_2\dots\tau_{m-1} f = \dots = \tau_1\tau_2 f = \tau_1 f = f$.

5. Show by induction that if $\sigma f = f$ then $\forall k \in \mathbb{N} \sigma^k f = f$.

Answer. Base case: $k = 1$. By hypothesis, $\sigma f = f$.

IH: For some k , $\sigma^k f = f$.

IS: $\sigma^{k+1} f = \sigma \sigma^k f = \sigma f$ (by IH). And by hypothesis, $\sigma f = f$.

[Remark: I will not deliberately test you on induction for its own sake, but might ask you to use induction on the way to proving something interesting.]

6. Show that if (G, \circ) is a group then $g \circ h = g \circ h'$ iff $h = h'$.¹

Answer. $g \circ h = g \circ h'$ iff $g^{-1} \circ g \circ h = g^{-1} \circ g \circ h'$ iff $h = h'$.

¹ \circ is just a group operation, it need not be composition.