ALGEBRA FINAL

Originality and a feeling of one's own dignity are achieved only through work and struggle. – Dostoyevsky

No books or notes. Problems marked (−) are relatively easy while those marked (*) are particularly challenging. Maximal Grade 200.

DO THREE OF PROBLEMS 1,2,3,4

1. (15) Assume as a fact that when \( p \) is a prime \( \mathbb{Z}_p^* \) is cyclic. Assume as a fact that 77003 is prime. How many \( x \in \mathbb{Z}_{77003}^* \) satisfy \( x^7 = 2? \) (You must give a clear reason for your answer!)

Solution: One. Let \( g \) be a generator so \( 2 = g^i \) for some \( i \). We want \( x = g^y \) so that \( g^{7y} = g^i \) which means \( 7y \equiv i \mod 77002 \). As 7,77002 are relatively prime this has a unique solution.

2. (15) Let \( G \) be a group and \( a \in G \). Define

\[
X(a) = \{g \in G : ga = ag\}
\]

What is \( X(a) \) usually called? Prove that \( X(a) \) is a subgroup of \( G \).

Solution: Normalizer, or Centralizer.

(a) Identity: As \( ea = ae, e \in X(a) \).
(b) Product: Let \( g_1, g_2 \in X(a) \). Then

\[
(g_1g_2)a = g_1(g_2a) = g_1(ag_2) = (g_1a)g_2 = (ag_1)g_2 = a(g_1g_2)
\]

so \( g_1g_2 \in X(a) \).
(c) Inverse: Let \( g \in X(a) \). So \( ga = ag \). Left and right multiplying by \( g^{-1} \) gives \( ag^{-1} = g^{-1}a \) so \( g^{-1} \in X(a) \).

3. (15) Give the definition of \( H \) being a normal subgroup of \( G \). (You can assume that subgroup has already been defined.) Is the group of \( n \times n \) real matrices of determinant one a normal subgroup of the group of \( n \times n \) nonsingular real matrices? Why?

Solution: Definition: If \( h \in H \) and \( g \in G \) then \( g^{-1}hg \in H \).

Yes, it is a normal subgroup. Let \( B \) have \( det(B) = 1 \) and let \( A \) be nonsingular, then

\[
det(A^{-1}BA) = det(A)^{-1}det(B)det(A) = 1
\]

so \( A^{-1}BA \) is in the subgroup.
4. (15) Let $F,K$ be fields with $F \subset K$ and $[K:F] = 13$. Let $\alpha \in K$ with $\alpha \notin F$. Show that $\alpha$ satisfies a polynomial $p(x) \in F[x]$ of degree 13. Further, show that $\alpha$ satisfies a minimal polynomial $p(x) \in F[x]$ of degree 13.

Solution: As $1, \alpha, \ldots, \alpha^{13}$ are independent there are $a_0, \ldots, a_{13} \in F$, not all zero, with $\sum_{i=0}^{13} a_i \alpha^i = 0$. Set $p(x) = \sum_{i=1}^{13} a_i x^i$. If $\alpha$ satisfies a minimal polynomial of degree $n$ then $[F(\alpha) : F] = n$ but $F(\alpha) \subset K$ so $n|13 = [K:F]$. We can’t have $n = 1$ as $\alpha \notin F$ so $n = 13$.

DO ALL PROBLEMS IN THIS SECTION

5. (25) Define the terms Integral Domain and Field. (You may assume the term Ring has been defined so you need only give the additional properties. Prove that a finite Integral Domain is a Field.

Solution: An Integral Domain has the property that $xy = 0$ implies $x = 0$ or $y = 0$. A Field has the property that if $a \neq 0$ there exists $b$ with $ab = 1$. Say $D = \{x_1, \ldots, x_s\}$ is a finite Integral Domain and let $a \neq 0$. Consider $ax_1, \ldots, ax_s$. If two were equal we would have $ax_i = ax_j$ so $a(x_i - x_j) = 0$, contradicting the Integral Domain property. So they are all distinct, by the PigeonHole principle they have all values in $D$, including 1, so some $ax_i = 1$.

6. (20) Let $G$ be an Abelian Group under multiplication and define $\phi : G \rightarrow G$ by $\phi(x) = x^3$. Show that $\phi$ is a homomorphism. Now assume further that $G$ is a finite group and that $o(G)$ is not divisible by 3. Show that $\phi$ is a bijection.

Solution: $\phi(xy) = (xy)^3 = x^3 y^3 = \phi(x)\phi(y)$. If $\phi(x) = e$ then $x^3 = e$ so either $x = e$ or $x$ has order 3, but as 3 doesn’t divide $o(G)$ we can’t have order 3 (Lagrange’s Theorem). That is, $\phi$ is injective. But as $G$ is finite this means $\phi$ is a bijection.
7. (25) With $D_{10}$ as given in the attached sheet:

(a) (-)(5) What is the inverse of $R2$?
Solution: $R4$

(b) (10) Find the conjugacy class of $R3$.
Solution: We look at all $X \cdot R3 \cdot X^{-1}$. For $X = \{e, R1, R2, R3, R4\}$ we get $R3$. For $X = F_i$, which is self-inverse, we get $F_iR3F_i$ which is always $R2$. So the answer is $\{R3, R2\}$.

(c) (5) Find $(R3)^{201}$.
Solution: As $R3$ has order five, $(R3)^{201} = R3$.

(d) (-)(5) Is $D_{10}$ Abelian? Give a short reason.
Solution: No, for example $R1 \cdot F_0 \neq F_0 \cdot R1$.

8. (20) Factor $2^3 \cdot 3 \cdot 5 \cdot 13$ into primes in $\mathbb{Z}[i]$. Prove that if $p = 4k + 3$ is a prime then it is a Gaussian prime.

Solution: We factor each factor into primes:

$$2^3 \cdot 3 \cdot 5 \cdot 13 = (-1)(1 + i)^6 \cdot 3(2 + i)(2 - i)(3 + 2i)(3 - 2i)$$

For the second, if $p = \alpha \beta$ then $p^2 = d(p) = d(\alpha)d(\beta)$ so $d(\alpha) = p$. With $\alpha = x + iy$ this would mean $x^2 + y^2 = p$ but the sum of two squares can never be three modulo four.

9. (20) This problem concerns finite Abelian Groups.

(a) (5) State the Fundamental Theorem for finite Abelian Groups, the result that describes all such groups.
Solution: Every Finite Abelian Group can be expressed as the product of cyclic groups.

(b) (5) How many elements of $\mathbb{Z}_5 \times \mathbb{Z}_{25}$ have order 5?
Solution: All $(x, y)$ with $0 \leq x \leq 4$ and $y \in \{0, 5, 10, 15, 20\}$, which is 25 elements, except $(0, 0)$, so 24.

(c) (10) List the Abelian Groups with precisely 100 elements. (Your list should have every such group but each group only once.)
Solution: There are four:

i. $Z_2 \times Z_2 \times Z_5 \times Z_5$
ii. $Z_4 \times Z_5 \times Z_5$
iii. $Z_2 \times Z_2 \times Z_{25}$
iv. $Z_4 \times Z_{25}$

10. (-)(10) In $\mathbb{Z}[i]$ is $9 + 4i \in (2 + i)$? Give your reason!
Solution: $
\frac{9 + 4i}{2 + i} = \frac{9 + 4i(2 - i)}{2 + i(2 - i)} = \frac{22 - i}{5} \notin \mathbb{Z}[i]
$
so: NO!

11. (35) This problem concerns the finite field (you do not need to prove it is a field!)

$$F = \mathbb{Z}_7[x]/(x^3 + 5)$$
(a) (5) Describe the elements of $F$. How many are there?
Solution: $a + bx + cx^2$ with $a, b, c \in \mathbb{Z}_7$, giving 343 elements.
(b) (5) Find $(x^2 + 3)(x^2 + 4)$.
Solution: As $x^3 = -5 = 2$, $x^4 = 2x$ so
\[ (x^2 + 3)(x^2 + 4) = x^4 + 5 = 2x + 5 \]
(c) (5) Find the multiplicative inverse of $x$.
Solution: As $x(x^2) = 2$ we have $x(4x^2) = 4 \cdot 2 = 1$ so the inverse in $4x^2$.
(d) (10) Find all solutions, and show that they are all solutions, to the equation $y^6 = 1$ in $F$.
Solution: The solutions are $y = 1, 2, 3, 4, 5, 6$ as $\mathbb{Z}_7$ is a subfield of $F$. These are six solutions and there can be at most six (the degree of the polynomial) solutions, so that's all the solutions.
(e) (10) (*) Find $(x + 1)^{3420003}$.
Solution: As $F^\ast$ has 342 elements $(x + 1)^{342} = 1$ so
\[ (x + 1)^{3420003} = (x + 1)^3 = x^3 + 3x^2 + 3x + 1 = 3x^2 + 3x + 3 \]

It’s not what you don’t know that hurts you.
It’s what you know that just ain’t so.
– Satchel Paige
The Dihedral Group $D_{10}$ is the group of symmetries of the regular 5-gon. We imagine the vertices of the regular 5-gon labelled 0, 1, 2, 3, 4 in counterclockwise direction.

The symmetries come in three forms:

1. $R_i, i = 1, 2, 3, 4$. This is a rotation by $i$ notches in the counterclockwise direction.

2. $F_i, i = 0, 1, 2, 3, 4$. This is a flip around point $i$.

3. The identity $e$.

A Table for the Dihedral Group $D_{10}$.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
<th>R4</th>
<th>F0</th>
<th>F1</th>
<th>F2</th>
<th>F3</th>
<th>F4</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>R1</td>
<td>R2</td>
<td>R3</td>
<td>R4</td>
<td>F0</td>
<td>F1</td>
<td>F2</td>
<td>F3</td>
<td>F4</td>
</tr>
<tr>
<td>R1</td>
<td>R1</td>
<td>R2</td>
<td>R3</td>
<td>R4</td>
<td>e</td>
<td>F2</td>
<td>F3</td>
<td>F4</td>
<td>F0</td>
<td>F1</td>
</tr>
<tr>
<td>R2</td>
<td>R2</td>
<td>R3</td>
<td>R4</td>
<td>e</td>
<td>R1</td>
<td>F4</td>
<td>F0</td>
<td>F1</td>
<td>F2</td>
<td>F3</td>
</tr>
<tr>
<td>R3</td>
<td>R3</td>
<td>R4</td>
<td>e</td>
<td>R1</td>
<td>R2</td>
<td>F1</td>
<td>F2</td>
<td>F3</td>
<td>F4</td>
<td>F0</td>
</tr>
<tr>
<td>R4</td>
<td>R4</td>
<td>e</td>
<td>R1</td>
<td>R2</td>
<td>R3</td>
<td>F3</td>
<td>F4</td>
<td>F0</td>
<td>F1</td>
<td>F2</td>
</tr>
<tr>
<td>F0</td>
<td>F0</td>
<td>F1</td>
<td>F3</td>
<td>F4</td>
<td>F2</td>
<td>e</td>
<td>R2</td>
<td>R4</td>
<td>R1</td>
<td>R3</td>
</tr>
<tr>
<td>F1</td>
<td>F1</td>
<td>F4</td>
<td>F2</td>
<td>F0</td>
<td>F3</td>
<td>R3</td>
<td>e</td>
<td>R2</td>
<td>R4</td>
<td>R1</td>
</tr>
<tr>
<td>F2</td>
<td>F2</td>
<td>F0</td>
<td>F3</td>
<td>F1</td>
<td>F4</td>
<td>R1</td>
<td>R3</td>
<td>e</td>
<td>R2</td>
<td>R4</td>
</tr>
<tr>
<td>F3</td>
<td>F3</td>
<td>F1</td>
<td>F4</td>
<td>F2</td>
<td>F0</td>
<td>R4</td>
<td>R1</td>
<td>R3</td>
<td>e</td>
<td>R2</td>
</tr>
<tr>
<td>F4</td>
<td>F4</td>
<td>F2</td>
<td>F0</td>
<td>F3</td>
<td>F2</td>
<td>R2</td>
<td>R4</td>
<td>R1</td>
<td>R3</td>
<td>e</td>
</tr>
</tbody>
</table>