FINAL EXAM, HISTORY 0F MATH
DECEMBER 16, 2018

Question 1: *Points in $\mathbb{CP}^2$:* **Pts 10:** Suppose you know that a homogenous polynomial $p(x, y, z)$ a zero

$$(x_0, y_0, z_0) = \Big(\frac{15}{8}, \frac{21}{10}, \frac{27}{32}\Big).$$

Find a point (x', y', z') that represents the same point of projective 2-space for which $x', y', z' \in \mathbb{Z}$ have greatest common divisor 1.

Answer:(x_0, y_0, z_0) represents the collection $\{a(x_0, y_0, z_0) \mid a \in \mathbb{C}\} \in \mathbb{CP}^2$. Find $a \in \mathbb{Q}$, for which $a(x_0, y_0, z_0) = (x', y', z')$ has the desired properties. Here $a = \frac{\text{lcm}(8,10,32)}{3} = \frac{5\cdot 32}{3}$ produces $(x', y', z') = (25 \cdot 4, 7 \cdot 16, 9 \cdot 5)$ as desired.

Question 2: *Index of elements in S_n:* Suppose you have r elements $g_1, \dots, g_r$ (different from 1) in S_5, $g_1 = (1\,2\,3\,4\,5)$ and the following conditions hold:

- The sum of their indexes is 8;[1]
- All are 5-cycles; and
- The product $g_1 g_2 \cdots g_r$ is 1.

2.a **Pts 10:** What are the possibilities for r and such elements?

2.b **Pts 10:** Give an example of $P(y)$ so that $P(y) - x = 0$ would produce these elements as permutations in generating the Galois group of the equation $\{(x, y) \in \mathbb{C}^2 \mid P(y) - x = 0\}$.

Answer:*For 2.a:* A 5-cycle has index 4. So, the sum of the indices is $r \cdot 4 = 8 \implies r = 2$. From product 1, $g_2 = g_1^{-1}$.

For 2.b: An example of $P(y)$ giving such g_1 and g_2 is $P(y) = y^5$, from the branch points $x_1 = 0$ and $x_2 = \infty$.

Question 3: *Multiplying elements in S_n* **Pts 20:** What elements $g' \in S_5$ commute with $g_1 = (1\,2\,3\,4\,5)$? Write the effect of g' on i as a function of $g'(1)$.[2]

Answer: From the hint, apply $gg_1 = g_1 g$ to 1: $1 \mapsto g(2)$ from the left side; $g(1) \mapsto g(1) + 1$ from the right side. Therefore $g(2) = g(1) + 1$. Now apply both sides to 2: $2 \mapsto g(3)$ from the left side, and $g(2) \mapsto g(2) + 1$ from the right side. Therefore $g(3) = g(2) + 1$, etc. Therefore, whatever is $g(1)$, $g(i) = g(1) + i$.

[1]The index of $g \in S_n$ is n minus the number of disjoint cycles in the representation of g.

[2]Hint: From $gg' = g'g$ figure what g' does to 1, then to 2, etc.

Question 4: *Perspective from a point:* Here are three lines going through the point $(1,2) \in \mathbb{R}^2$:

$$L_1 = \{(1,2) + m_1(0,1) \mid m_1 \in \mathbb{R}\}$$
$$L_2 = \{(1,2) + m_2(1,1) \mid m_2 \in \mathbb{R}\}$$
$$L_3 = \{(1,2) + m_3(3,1) \mid m \in \mathbb{R}\}.$$

Take $P_1 = (1,3) \in L_1$ and $P_2 = (1+m_2, 2+m_2) \in L_2$.

4.a **Pts 15:** Set up finding the point P_3 (as a function of m_2) that lies on L_3 and the line, L_4, that contains P_1 and P_2 as two equations in two unknowns, with coefficients as functions of m_2.[3]

4.b **Pts 5:** Why would our text say that P_1, P_2, P_3 are in perspective with $(1,3), (2,3), (4,3)$ from $(1,2)$?

Answer: *For 4.a:* The line through P_1 and P_2 is given by points on

$$L_4 = \{(1,3) + m(P_2 - (1,3) = (1,3) + m(m_2, m_2 - 1) \mid m \in \mathbb{R}\}.$$

To find the value of m or m_3 that gives P_3 solve for it in the equation

$$m(m_2, m_2 - 1) = (1,2) + m_3(3,1) \text{ giving the meeting point of } L_3 \text{ and } L_4.$$

The equation would be $\begin{pmatrix} m_2 & -3 \\ m_2 - 1 & -1 \end{pmatrix} \begin{pmatrix} m \\ m_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

For 4.b: The points $(1,3), (2,3), (4,3)$ all lie on a line $y = 3$, that are meetings, respectively, with L_1, L_2, L_3. Any other three points, like P_1, P_2, P_3 are in perspective from $(1,2)$ with them if they also lie on a line meeting L_1, L_2, L_3.

Question 5: *Roots of 1.* In class we learned that Galois's group for the field generated by $e^{\frac{2\pi i}{p^u}}$ – with $u > 1$ a positive integer and p an odd prime – consists of the group $(\mathbb{Z}/p^u)^*$, the integers *not* divisible by p, $\mod p^u$ under multiplication.

5.a **Pts 10:** If m is an element in any group G for which $m^k = 1$, $k > 0$, show its order, $\text{ord}(m)$, (minimal positive power equal to 1) divides k.[4]

5.b **Pts 10:** Show $m = 1 + p$ gives an element of order p^{u-1}.[5]

5.c **Pts 5:** Suppose m' is a generator of $(\mathbb{Z}/p^u)^*$. Find k so that $(m')^k$ has order exactly $p - 1$.[6]

5.d **Pts 5:** Why does 5.c show that if m'' is an integer that generates $(\mathbb{Z}/p)^*$, it may not generate $(\mathbb{Z}/p^2)^*$?

Answer: *For 5.a:* Write $s \cdot \text{ord}(m) + t \cdot k = \gcd(m,k) \stackrel{\text{def}}{=} v$. Then,

$$m^{s \cdot \text{ord}(m) + t \cdot k} = 1, \text{ so } v \text{ divides } \text{ord}(m).$$

By definition of $\text{ord}(m)$, v equals it.

For 5.b: Expand $(1+p)^{p^{u-1}} \mod p^u$ by the binimial theorem to get

$$1 + p^{u-1}p + \frac{p^{u-1}(p^{u-1} - 1)}{2} p^2 + \cdots \equiv 1 \mod p^u.$$

---

[3] Don't bother to solve the equations.

[4] Apply the Euclidean algorithm to the pair $(\text{ord}(m), k)$.

[5] Hint: Use the binomial theorem to show the minimal power of m that is $1 \mod p^u$ is p^{u-1}.

[6] 1st give the order of $(\mathbb{Z}/p^u)^*$, which then is the order of m'.

From 5.a, the order of m' divides p^{u-1}. In the binomial expansion replace p^{u-1} by p^l with $l < u-1$. You see the 2nd term is not $\equiv 0 \mod p^u$. It cannot be canceled by any other terms.

For 5.c: The number of elements $\mod p^u$ divisible by p is p^{u-1}. So the order of $(\mathbb{Z}/p^u)^*$ is $p^{u-1}(p-1)$. Then, $(m')^{p^{u-1}}$ has order $p-1$, as asked for.

For 5.d: Because if $m'' \mod p^u$ has order $p-1$, as is always possible from 5.c, it cannot generate the whole group $(\mathbb{Z}/p^2)^*$ of order $p^u - p^{u-1}$.

Question 6: *Using a higher box principle.* **Pts 20:** Suppose α is a real algebraic number, a zero of an irreducible polynomial $F(y) \in \mathbb{Z}[y]$, with $\deg(F) = d$. Homogonize to get $x^d F(\frac{y}{x}) = f(x,y)$. In class we heard that the Thue-Siegel-Roth Theorem considers any $\epsilon > 0$. It says, for some constant $C(\epsilon, d) = C$,

$$|f(x,y)| > \max(|x|,|y|)^{d-2-\epsilon} \text{ for } x, y \in \mathbb{Z}, \max(|x|,|y|) > C.$$

Suppose $g(x,y) \in \mathbb{Z}[x,y]$ has total degree, $\deg(g) < d-2$. Why does this show $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid f(x,y) - g(x,y) = 0\}$ is finite?[7]

Answer: Choose ϵ in the Thue-Siegel-Roth theorem very small. Then,

$$|f(x,y) - g(x,y)| \geq |f(x,y)| - |g(x,y)| \geq \max(|x|,|y|)^{d-2-\epsilon} - D\max(|x|,|y|)^{\deg(g)}.$$

Then, for $\max(|x|,|y|)$ large the second term is smaller than the first term:

$f(x,y) - g(x,y) \neq 0$ for $\max(|x|,|y|)$ large; it has finitely many integer solutions.

[7]You may use without proof that if $\max(|x|,|y|)$ is large, then there is a constant D such that $|g(x,y)| < D\max(|x|,|y|)^{\deg(g)}$.