Yunzhe Zheng. (2025/04/02)

Problem 1. *Decompose $x^9 - x$ into a product of monic irreducible polynomials over $\mathbb{F}_3$.*

Solution: $x^9 - x = x(x^8 - 1) = x(x-1)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x-1)(x+1)(x^2+1)(x^2+2x+2)(x^2+x+2)$ in $\mathbb{F}_3$.

Problem 2. *What is the product of all elements of the multiplicative group $\mathbb{F}_{29}^*$.*

Solution: Consider symmetric group S_{29}, since 29 is prime, we notice that there are 28! elements of order 29 (they are all of the form $(a_1, a_2, \ldots, a_{29})$, and we can fix a_1 to be 1 and permute other entries, which gives us 28!). Since for each 29-group (automatically Sylow 29-group), it has $29-1 = 28$ elements of order 29 (excluding 1), then there are $(p-2)!$ Sylow 29-group in S_{29}, then by Sylow Third theorem, $(29-2)! \equiv 1 \mod 29$, then $(29-1)! \equiv 28 \mod 29$, which implies that product of all elements in $\mathbb{F}_{29}^*$ is -1.

Problem 3. *Find two first primes which remain primes in the rings of algebraic integers in the fields $\mathbb{Q}[i]$ and $\mathbb{Q}[s]$ where $s^2 = -5$.*

Solution: Since $i^2 = -1 \equiv 3 \mod 4$ and $-5 \equiv 3 \mod 4$, then from Artin's Algebra Theorem 13.6.1(c), it is sufficient to find prime integer p and check whether -1 and -5 are square modulo p, which is, by the Euler criterion, equivalent to checking $(-1)^{\frac{p-1}{2}} \equiv -1 \mod p$ and $(-5)^{\frac{p-1}{2}} \equiv -1 \mod p$. From calculation, the first two integer primes satisfying that equality are $11, 19$.

Problem 4. *Find all irreducible polynomials of degree 3 over $\mathbb{F}_4$.*

Solution: $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, and since polynomial of degree 3 is irreducible if and only if it has no root in $\mathbb{F}_4$, by enumerating all possibilities on the coefficients, we obtain all such possibilities: x^3+1, $x^3+\alpha$, $x^3+\alpha+1$, x^3+x+1, $x^3+\alpha x+1$, $x^3+(\alpha+1)x+1$, x^3+x^2+1, $x^3+x^2+x+\alpha$, $x^3+x^2+\alpha x+\alpha+1$, $x^3+x^2+(\alpha+1)x+\alpha$, $x^3+\alpha x^2+1$, $x^3+\alpha x^2+x+\alpha+1$, $x^3+\alpha x^2+\alpha x+\alpha$, $x^3+\alpha x^2+(\alpha+1)x+\alpha$, $x^3+\alpha x^2+(\alpha+1)x+(\alpha+1)$, $x^3+(\alpha+1)x^2+1$, $x^3+(\alpha+1)x^2+x+\alpha$, $x^3+(\alpha+1)x^2+\alpha x+\alpha$, $x^3+(\alpha+1)x^2+\alpha x+\alpha+1$, $x^3+(\alpha+1)x^2+(\alpha+1)x+\alpha+1$.

Problem 5. *Find solvable subgroups of S_6 with transitive action on 6 points. (As many as you can modulo isomorphism).*

Solution: 1. C_6 is a subgroup acting transitively on 6 points which is obviosuly solvable because it is abelian.

2. $D_6 \subseteq S_6$ acts transitively on 6 points since it characterizes rotations and flips of a hexagon. Consider the sequence $D_6 \supset C_6 \supset \{e\}$, then D_6/C_6 has prime order, thus is

abelian. C_6 is abelian, hence D_6 is solvable.

3. S_3 acts transitively on itself, which has 6 points. It is solvable by considering the sequence $S_3 \supseteq A_3 \supseteq \{e\}$, where S_3/A_3 is abelian since has order 2, and A_3 is abelian.

4. A_4 acts transitively on itself, which has 12 elements, then by taking a subgroup of order 2 in A_4, say $\langle(1\ 2)(3\ 4)\rangle$, we obtain 6 left (right) coset of A_4, and surely A_4 act transitively on these cosets. Also, A_4 is solvable by considering a normal subgroup of order 4 in A_4, namely $S := \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \mathrm{Id}\}$. Notice that S itself is abelian, and A_4/S is abelian since it has prime order.

5. S_4 acts tranitively on 6 points by the same reasoning as before, but pick a subgroup of order 4 in S_4, say $\langle(1\ 2), (3\ 4)\rangle$. S_4 is also solvable by considering the similar sequence $S_4 \supseteq A_4 \supseteq S \supseteq \{e\}$, where A_4 is normal in S_4 because it has index 2, and thus S_4/A_4 is abelian.