HW 10

1. If G is a finite group with $|G| = n$, then we can think of G as a subgroup of S_n using the action of G on itself by left multiplication. I.e. if $G = \{g_1, g_2, \ldots, g_n\}$, left multiplication by an element of G gives a bijection from G to itself. (See HW8, Q1 from 361 for related info). So $G \leq S_n$

For F a field with $\mathrm{char}(F) = 0$, let $K = F(y_1, \cdots, y_n)$ where the y_i are transcendental over F, and let $E \subseteq K$ where $E = F(s_1, s_2, \ldots, s_n)$ is the subfield generated by the elementary symmetric functions. $G(K/E) = S_n$, since an automorphism of K fixing E is determined by where the y_i get ~~set~~ sent, but the y_i are the roots of the polynomial

$$f(x) = (x-y_1)(x-y_2) \cdots (x-y_n),$$ and K is the splitting field of $f(x)$ over E. K is also separable over E, since $\mathrm{char}(E) = 0$. Any permutation of the y_i's induces an automorphism of K that fixes E.

Now think of G as a subgroup of $G(K/E)$ and let L be the subfield $E \subseteq L \subseteq K$ fixed by G. By the main theorem of Galois theory, $L \subseteq K$ is a finite normal extension, and $G(K/L) = G$.

2. a. Since $x^3 - 4x^2 + 6x - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ we know (by expanding the RHS and comparing coefficients) that $-\alpha_1 - \alpha_2 - \alpha_3 = -4$, so the minimal polynomial of $\alpha_1 + \alpha_2 + \alpha_3$ is $x - 4$

b. With the same expansion as in part a., we know

$$x^3 - 4x^2 + 6x - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

$$= x^3$$

$$+ (-\alpha_1 - \alpha_2 - \alpha_3)x^2$$

$$+ (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x$$

$$+ (-\alpha_1\alpha_2\alpha_3),$$

so

$$-\alpha_1 - \alpha_2 - \alpha_3 = -4 \Rightarrow \overbrace{\alpha_1 + \alpha_2 + \alpha_3}^{s_1} = 4$$

$$\overbrace{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3}^{s_2} = 6$$

$$-\alpha_1\alpha_2\alpha_3 = -2 \Rightarrow \overbrace{\alpha_1\alpha_2\alpha_3}^{s_3} = 2$$

Then the polynomial $(x-\alpha_1^2)(x-\alpha_2^2)(x-\alpha_3^2)$ is cubic, with the desired roots, and it expands as

$$= x^3$$

$$+ (-\alpha_1^2 - \alpha_2^2 - \alpha_3^2)x^2$$

$$+ (\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2)x$$

$$+ (-\alpha_1^2\alpha_2^2\alpha_3^2)$$

The constant term is $-s_3^2 = -4$.

The coeff on x is $s_2^2 - 2s_1s_3 = 36 - 16 = 20$

The coeff on x^2 is $-(s_1^2 - 2s_2) = -4$.

So the desired polynomial is $x^3 - 4x^2 + 20x - 4$.

3. $0 \lneq 60\mathbb{Z} \lneq 20\mathbb{Z} \lneq \mathbb{Z}$

has quotients infinite cyclic, cyclic of order 3, cyclic of order 20.

$0 \lneq 245\mathbb{Z} \lneq 49\mathbb{Z} \lneq \mathbb{Z}$ has quotients:

infinite cyclic, cyclic of order 5, cyclic of order 49.

Note that, if $n\mathbb{Z}$ is the subgp of $\mathbb{Z}$ gen by n and $k \cdot n$ is a multiple of n, then $k \cdot n\mathbb{Z}$ is a subgp of $n\mathbb{Z}$, and $n\mathbb{Z}/kn\mathbb{Z}$ is cyclic of order k.

So we can build isomorphic refinements:

$$0 \leq 14700\mathbb{Z} \leq 300\mathbb{Z} \leq 60\mathbb{Z} \leq 20\mathbb{Z} \leq \mathbb{Z}$$

$$0 \leq 14700 \leq 735\mathbb{Z} \leq 245\mathbb{Z} \leq 49\mathbb{Z} \leq \mathbb{Z}$$

both these comp series have quotients:

$$\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/20\mathbb{Z},\ \mathbb{Z}/49\mathbb{Z},$$

(in some order) so they're isomorphic.

b. the quotients of $0 \leq \langle 3 \rangle \leq \mathbb{Z}/24\mathbb{Z}$

are cyclic, order 8: $\{0, 3, 6, 9, 12, 15, 18, 21\}$ cyclic, order 3

the quotients of $0 \leq \langle 8 \rangle \leq \mathbb{Z}/24\mathbb{Z}$

are $\{0, 8, 16\}$: cyclic of order 3 cyclic, order 8.

so theyre already isomorphic.

4. the subgroup diagram of $\mathbb{Z}/48\mathbb{Z}$ looks like

$$\begin{tikzcd}[column sep=small]
 & & & & \mathbb{Z}/48\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
 & & & \langle 2 \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 3 \rangle \arrow[dl, dash] \\
 & & \langle 4 \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 6 \rangle \arrow[dl, dash] & \\
 & \langle 8 \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 12 \rangle \arrow[dl, dash] & & \\
\langle 16 \rangle \arrow[dr, dash] & & \langle 24 \rangle \arrow[dl, dash] & & & \\
 & \langle 0 \rangle & & & &
\end{tikzcd}$$

we find composition series by repeatedly choosing <u>maximal</u> subgroups, descending from $\mathbb{Z}/48\mathbb{Z}$ to $\langle 0 \rangle$:

$$0 \leq 16 \leq 8 \leq 4 \leq 2 \leq \mathbb{Z}/48\mathbb{Z}$$
$$0 \leq 24 \leq 8 \leq 4 \leq 2 \leq \mathbb{Z}/48\mathbb{Z}$$
$$0 \leq 24 \leq 12 \leq 4 \leq 2 \leq \mathbb{Z}/48\mathbb{Z}$$
$$0 \leq 24 \leq 12 \leq 6 \leq 2 \leq \mathbb{Z}/48\mathbb{Z}$$
$$0 \leq 24 \leq 12 \leq 6 \leq 3 \leq \mathbb{Z}/48\mathbb{Z}$$

5.a. Any $\sigma \in S_n$ can be written as a product of disjoint cycles. any n-cycle $(a_1\ a_2\ \cdots\ a_n)$ can be written as

$$(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n)\cdots(a_1\ a_3)(a_1\ a_2)$$

So any $\sigma \in S_n$ can be written as a product of transpositions.

b.
$$\begin{aligned}(1\,2\,3\,4\,5) &= (15)(14)(13)(12)\\ &= (12)(12)(15)(14)(13)(12)\\ &= (15)(32)(43)(14)\end{aligned}$$

c. (non-standard proof). Let

$$f(x) = \prod_{1\le i<j\le n}(x_i - x_j)$$, a polynomial in variables $\{x_1 \dots x_n\}$ and with $\mathbb{Q}$-coefficients.

Let $X = \{f(x), -f(x)\}$.

S_n acts on X by $\sigma\cdot f(x) = \prod_{1\le i<j\le n}(x_{\sigma(i)} - x_{\sigma(j)})$,

(which is just $f(x)$ times some number of minus signs)

and $\sigma\cdot(-f(x)) = -\sigma\cdot f(x)$.

The identity (1) satisfies $(1)\cdot f(x) = f(x)$

$(1)\cdot -f(x) = -f(x)$.

and from the definition we can confirm that

$$\sigma\circ\tau\cdot f(x) = \sigma\cdot(\tau\cdot f(x))$$

$\forall\ \sigma, \tau \in S_n$. So this is a group action.

Think about how the transposition $\tau = (a\ b)$ acts ($a<b$)

on $\prod_{1\le i<j\le n} (x_i - x_j)$.

if neither i nor j is a or b, then the factor

$(x_i - x_j)$ is unchanged by τ.

if $i=a$, $j\neq b$, and $j<b$, then $(x_a - x_j)$ becomes $(x_b - x_j) = -(x_j - x_b)$ — there are $b-a-1$ such factors

if $i\neq a$, $j=b$, and $a<i$, then $(x_i - x_b)$ becomes $(x_i - x_a) = -(x_a - x_i)$ — there are $b-a-1$ such factors

if $i=a$, $j=b$ then $(x_a - x_b)$ becomes $(x_b - x_a) = -(x_a - x_b)$. — there is one such factor.

if $i = a$, $j > b$ or if $i < a$, $j = b$ then

$(x_i - x_j)$ is changed, but a minus sign is not

introduced.

in total, $\tau = (a\,b)$ acts on $f(x)$ by multiplying

it by $2(b-a-1)+1$ factors of -1.

so $\tau = (a\,b)$ acts on X by
$$\tau \cdot f(x) = -f(x)$$
$$\tau \cdot (-f(x)) = f(x).$$

so pick $\sigma \in S_n$, and write its as a product

of transpositions
$$\sigma = \tau_1 \cdots \tau_n$$
$$= \rho_1 \cdots \rho_m.$$

if $\sigma \cdot f(x) = f(x)$, then n, m must both

be even.

if $\sigma \cdot f(x) = -f(x)$, then n, m must both

be odd.

d. ~~Conjugation preserves cycle structure~~ if σ is

an even permutation and τ is any permutation,

then
$$\tau \circ \sigma \circ \tau^{-1} \cdot f(x) = \tau \circ \sigma \cdot (\tau^{-1} \cdot f(x))$$
$$= \tau \circ \tau^{-1} \cdot f(x) = f(x) \; [\text{or } (-1)^2 f(x).]$$

since $\tau\sigma\tau^{-1} \cdot f(x) = f(x)$, $\tau\sigma\tau^{-1}$ is even, so is in A_n

so A_n is a normal subgroup of S_n.

e. Removed from HW.