Paper Guide for 2010

"Donuts, pizzas and real good looking boys in Cairo."

—/—

Ansatz 1: Assume true that $Aut(K)$ is a non-empty set.

Ansatz 2: Assume true that for any $\alpha, \beta \in Aut(K)$ then the composition mapping $\alpha \circ \beta$ also belongs to $Aut(K)$.

$Aut(K)$ is the set of bijective homomorphism $\alpha : K \to K$.

Lets show that the group product of $Aut(K)$ is by composition:

$$\circ : Aut(K) \times Aut(K) \to Aut(K)$$

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)).$$

For associativity; composition is always associative by the associative axiom.

For identity; lets define the mapping:

$$Id_K : K \to K$$

$$Id_K(x) = x \quad \forall x \in K.$$

Lets prove that $Id_K \in Aut(K)$, obviously it is

bijective, lets show that Id_K is a homomorphism; for any $x_1, x_2 \in K$, take $Id_K(x_1x_2) = x_1x_2 = Id_K(x_1)\,Id_K(x_2)$. Hence $Id_K \in Aut(K)$ is true.

Lets show that Id_K is the identity of $Aut(K)$, for any $\alpha \in Aut(K)$, take:

$$(Id_K \circ \alpha)(x) = Id_K(\alpha(x))$$
$$= \alpha(x)$$
$$= \alpha(Id_K(x))$$
$$= (\alpha \circ Id_K)(x)$$

Hence Id_K is the identity for $Aut(K)$.

For inverse; let $\alpha \in Aut(K)$. Since α is bijective, there exist α^{-1} st

$$\alpha \circ \alpha^{-1} = Id_K = \alpha^{-1} \circ \alpha.$$

Lets show that $\alpha^{-1} \in Aut(K)$. Obviously α^{-1} is bijective. Lets show α^{-1} is a homomorphism.

Take: $\alpha(\alpha^{-1}(xy))$
$= xy.$ $\quad \forall x, y \in K$

Take: $\alpha(\alpha^{-1}(x)\alpha^{-1}(y))$
$= \alpha(\alpha^{-1}(x))\,\alpha(\alpha^{-1}(y))$
$= xy$ $\quad \forall x, y \in K.$

Hence: $\alpha(\alpha^{-1}(xy)) = \alpha(\alpha^{-1}(x)\alpha^{-1}(y))$

Since α is injective:

$\Rightarrow \alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y) \quad \forall x, y \in K$.

Hence α^{-1} is a homomorphism $\Rightarrow \alpha^{-1} \in Aut(K)$.
Hence $\forall \alpha \in Aut(K) \quad \exists \alpha^{-1} \in Aut(K)$ st
$\alpha \circ \alpha^{-1} = Id_K = \alpha^{-1} \circ \alpha$

Hence $\circ$ is the group product of $Aut(K)$.

—/—

Q, K groups, $\varphi: Q \to Aut(K)$ group homomorphism.

$K \times_\varphi Q$ is defined as follows

i) As the set $K \times_\varphi Q = K \times Q$.

ii) The multiplication $*$ on $K \times_\varphi Q$ is defined as:

$$*: (K \times Q) \times (K \times Q) \to (K \times Q)$$

$$(k_1, q_1) * (k_2, q_2) = (k_1 h(q_1)(k_2), q_1 q_2).$$

Lets show that $K \times_\varphi Q$ is a group.

Obviously $K \times_\varphi Q \neq \emptyset$ since $K \times_\varphi Q$ is defined as the set $K \times Q$.

Lets show that $*$ is the group product of $K \times_\varphi Q$

For associativity;

Take: $[(k_1, q_1) * (k_2, q_2)] * (k_3, q_3)$ for any $k_1, k_2, k_3 \in K$ and for any $q_1, q_2, q_3 \in Q$.

$= (k_1 \varphi(q_1)(k_2), q_1 q_2) * (k_3, q_3)$

$= (k_1 \varphi(q_1)(k_2) \varphi(q_1 q_2)(k_3), q_1 q_2 q_3)$

Since φ is a group homomorphism, hence

$\ldots = (k_1 \varphi(q_1)(k_2) \varphi(q_1)(\varphi(q_2)(k_3)), q_1 q_2 q_3)$

Take: $(k_1, q_1) * [(k_2, q_2) * (k_3, q_3)]$ for any $k_1, k_2, k_3 \in K$ and for any $q_1, q_2, q_3 \in Q$.

$= (k_1, q_1) * (k_2 \varphi(q_2)(k_3), q_2 q_3)$

$= (k_1 \varphi(q_1)(k_2 \varphi(q_2)(k_3)), q_1 q_2 q_3)$

Since $\varphi(q_1) \in Aut(K)$, $\varphi(q_1)$ is a homomorphism, hence

$\ldots = (k_1 \varphi(q_1)(k_2) \varphi(q_1)(\varphi(q_2)(k_3)), q_1 q_2 q_3)$

Hence:

$[(k_1, q_1) * (k_2, q_2)] * (k_3, q_3) = (k_1, q_1) * [(k_2, q_2) * (k_3, q_3)]$

Hence the product $*$ is associative.

For identity, lets show that $(1, 1)$ is the identity for $K \rtimes_\varphi Q$.

Take: $(k, q) * (1, 1)$ for any $k \in K$, $q \in Q$.

$= (k\varphi(q)(1), q)$

$= (k, q)$ since $\varphi(q)(1) = 1 \quad \forall q \in Q$.

Take: $(1,1) * (k,q)$ for any $k \in K, q \in Q$.

$= (1\varphi(1)(k), q)$

$= (k, q)$ since $\varphi(1)(k) = Id_K(k) = k \quad \forall k \in K$

Hence: $(1,1)*(k,q) = (k,q) = (k,q)*(1,1)$

Hence $(1,1)$ is the identity for $K \rtimes_\varphi Q$.

For inverse; lets show $(\varphi(q^{-1})(k^{-1}), q^{-1})$ is the inverse for (k,q) for any $q \in Q, k \in K$

Take: $(\varphi(q^{-1})(k^{-1}), q^{-1}) * (k,q)$

$= (\varphi(q^{-1})(k^{-1})\varphi(q^{-1})(k), q^{-1}q)$

$= (\varphi(q^{-1})(k^{-1})\varphi(q^{-1})(k), 1)$

Since $\varphi(q^{-1}) \in Aut(K)$, so $\varphi(q^{-1})$ is a homomorphism hence;

$\ldots = (\varphi(q^{-1})(k^{-1}k), 1)$

$= (\varphi(q)(1), 1)$

$= (1, 1)$ since $\varphi(q)(1) = 1 \quad \forall q \in Q$

Take: $(k,q) * (\varphi(q^{-1})(k^{-1}), q^{-1})$

$= (k\varphi(q)(\varphi(q^{-1})(k^{-1})), qq^{-1})$

$= (k\varphi(q)(\varphi(q^{-1})(k^{-1})), 1)$

Since φ is a group homomorphism, hence

$\ldots = (k\varphi(qq^{-1})(k^{-1}), 1)$

$= (k\varphi(1)(k^{-1}), 1)$

$= (kk^{-1}, 1)$ Since $\varphi(1)(k^{-1}) = Id_K(k^{-1})$.

$= (1, 1)$.

Hence:

$$(\varphi(q^{-1})(k^{-1}), q^{-1}) * (k, q) = (1, 1) = (k, q) * (\varphi(q^{-1})(k^{-1}), q^{-1})$$

Hence $\forall (k, q) \in K \times_\varphi Q \ \exists (k, q)^{-1} = (\varphi(q^{-1})(k^{-1}), q^{-1}) \in K \times_\varphi Q$ st $(k, q)^{-1} * (k, q) = (k, q)^{-1} * (k, q) = (1, 1)$

Hence $(\varphi(q^{-1})(k^{-1}), q^{-1})$ is the inverse in $K \times_\varphi Q$.

Hence $K \times_\varphi Q$ is a group;

$$K \times_\varphi Q = (K \times Q, *, (1, 1)).$$

i) $Aut(C_{14}) = \{\phi_i : \overline{(i, 14)} = 1\}$

$\Rightarrow Aut(C_{14}) = \{\phi_1, \phi_3, \phi_5, \phi_9, \phi_{11}, \phi_{13}\}$

Pick $\alpha = \phi_3$

So, $\alpha^2 = \phi_9$, $\alpha^3 = \phi_{13}$, $\alpha^4 = \phi_{11}$, $\alpha^5 = \phi_5$, $\alpha^6 = \phi_1$.

α generates $Aut(C_{14})$, hence:

$$Aut(C_{14}) \cong C_6$$

where $C_6 = \langle \alpha \mid \alpha^6 = 1 \rangle$.

ii) $\varphi : C_3 \longrightarrow Aut(C_{14})$.

Since $Aut(C_{14}) \cong C_6$, lets find all homomorphism $h : C_3 \to C_6$ where:

$$C_6 = \langle \alpha \mid \alpha^6 = 1 \rangle$$
$$C_3 = \langle \beta \mid \beta^3 = 1 \rangle$$

There exist a homomorphism $h : C_3 \to C_6$ where $h(\beta) = \alpha^r$ for some $1 \leq r \leq 6 \iff ord(\alpha^r) \mid 3$.

Take $ord(\alpha^r) \mid 3$

$$\Rightarrow ord(\alpha^r) = 1, 3$$

Case 1: $ord(\alpha^r) = 1$

$$\Rightarrow \frac{6}{HCF(r, 6)} = 1$$

$$\Rightarrow r = 6 \quad (\alpha^6 = 1).$$

Hence $h_0(\beta) = 1$ is a homomorphism.

Case 2: $\text{ord}(\alpha^r) = 3$

$$\Rightarrow \frac{6}{HCF(r,6)} = 3$$

$$\Rightarrow 2 = HCF(r,6)$$

$$\Rightarrow r = 2, 4.$$

Hence $h_1(\beta) = \alpha^2$, $h_2(\beta) = \alpha^4$ are homomorphisms.

Recall that $Aut(C_{14}) \cong C_6$ where $1 = \phi_1$, $\alpha^2 = \phi_9$, $\alpha^4 = \phi_{11}$. Hence all the homomorphisms $\varphi: C_3 \to Aut(C_{14})$ are:

$$\varphi_0(\beta) = 1$$
$$\varphi_1(\beta) = \phi_9$$
$$\varphi_2(\beta) = \phi_{11}$$

—/—

Ansatz: Suppose that if F and G are groups, G is abelian and F is non-abelian then $G \ncong F$.

Lets prove that $G \ncong F$, by contradiction suppose that $G \cong F$ $\Rightarrow$ there exist a homomorphism $\psi: G \to F$.

Since G is abelian, for all $x, y \in G$

$$xy = yx.$$

Take: $\psi(xy) = \psi(x)\psi(y)$

Take: $\psi(xy) = \psi(yx)$
$= \psi(y)\psi(x)$

Hence $\psi(x)\psi(y) = \psi(y)\psi(x)$ for all $\psi(x), \psi(y) \in F \Rightarrow F$ is ablican, this is a contradiction from the hypothesis. Hence $G \not\cong F$.

Lets find the distinct groups isomorphic to $C_{14} \rtimes_\varphi C_3$, for some homomorphism, $\varphi: C_3 \to Aut(C_{14})$, where:

$$C_3 = \langle \beta \mid \beta^3 = 1 \rangle$$
$$C_{14} = \langle \gamma \mid \gamma^{14} = 1 \rangle$$

Lets do the critical calculation for $C_{14} \rtimes_{\varphi_0} C_3$, $\varphi_0: C_3 \to Aut(C_{14})$.

Take $B = (1, \beta)$, $C = (\gamma, 1)$:

$$B * C = (1, \beta) * (\gamma, 1)$$
$$= (\varphi_0(\beta)(\gamma), \beta)$$
$$= (\varphi_1(\gamma), \beta)$$
$$= (\gamma, \beta)$$
$$= C * B.$$

Hence:
$C_{14} \rtimes_{\varphi_0} C_3 = \langle B, C \mid B^3 = C^{14} = 1, BC = CB \rangle$.

Lets do the critical calculation for $C_{14} \rtimes_{\varphi_1} C_3$, $\varphi_1 : C_3 \to Aut(C_{14})$.

Take $B = (1, \beta)$, $C = (\gamma, 1)$

$$B * C = (1, \beta) * (\gamma, 1)$$
$$= (\varphi_1(\beta)(\gamma), \beta)$$
$$= (\varphi_1(\gamma), \beta)$$
$$= (\gamma^9, \beta)$$
$$= C^9 * B$$

Hence:
$C_{14} \rtimes_{\varphi_1} C_3 = \langle B, C \mid B^3 = C^{14} = 1, \; BC = C^9 B \rangle$.

Lets do the critical calculation for $C_{14} \rtimes_{\varphi_2} C_3$, $\varphi_2 : C_3 \to Aut(C_{14})$

Take $B = (1, \beta)$, $C = (\gamma, 1)$

$$B * C = (1, \beta) * (\gamma, 1)$$
$$= (\varphi_2(\beta)(\gamma), \beta)$$
$$= (\varphi_{11}(\gamma), \beta)$$
$$= (\gamma^{11}, \beta)$$
$$= C^{11} * B.$$

Hence
$C_{14} \rtimes_{\varphi_2} C_3 = \langle B, C \mid B^3 = C^{14} = 1, \; BC = C^{11}B \rangle$

Observe that $ord(\beta) = ord(\beta^2) = 3$, hence β and β^2 can be considered as generators for C_3. Hence lets do a different critical calculation for $C_{14} \rtimes_{\varphi_2} C_3$, $\varphi_2 : C_3 \to Aut(C_{14})$.

Let $D = (1, \delta)$, $C = (\gamma, 1)$ where $\delta = \beta^2$.

$$\begin{aligned} D * C &= (1, \delta) * (\gamma, 1) \\ &= (\varphi_2(\delta)(\gamma), \delta) \\ &= (\varphi_2(\beta^2)(\gamma), \delta) \\ &= (\varphi_9(\gamma), \delta) \\ &= (\gamma^9, \delta) \\ &= C^9 * D \end{aligned}$$

Hence
$C_{14} \rtimes_{\varphi_2} C_3 = \langle D, C \mid D^3 = C^{14} = 1, \; DC = C^9 D \rangle$

Hence $C_{14} \rtimes_{\varphi_1} C_3 \cong C_{14} \rtimes_{\varphi_2} C_3$ since swiching the generators $\beta \leftrightarrow \beta^2$ gives the description.

Also $C_{14} \rtimes_{\varphi_0} C_3 \ncong C_{14} \rtimes_{\varphi_1} C_3$ since $C_{14} \rtimes_{\varphi_0} C_3$ is abliean and $C_{14} \rtimes_{\varphi_1} C_3$ is non-abliean.

Hence there are two distinct groups isomorphic to $C_{14} \rtimes_{\varphi} C_3$.

They are:

$C_{14} \rtimes_{\varphi_1} C_3 = \langle B, C \mid B^3 = C^{14} = 1,\ BC = C^9 B \rangle.$

$C_{14} \rtimes_{\varphi_0} C_3 = \langle B, C \mid B^3 = C^{14} = 1,\ BC = CB \rangle.$

— / ——

2) See paper guide for 2012, question 2 part of 4

— / —

Lets show for any $x, y \in X$ then either $\langle x \rangle \wedge \langle y \rangle = \emptyset$ or $\langle x \rangle = \langle y \rangle$.

It suffices to prove that if $\langle x \rangle \wedge \langle y \rangle \neq \emptyset$ then $\langle x \rangle = \langle y \rangle$.

If $\langle x \rangle \wedge \langle y \rangle \neq \emptyset \Rightarrow \exists k \in \langle x \rangle \wedge \langle y \rangle$.

Hence $k \in \langle x \rangle \Rightarrow k = g \circ x$ for some $g \in G$.
Hence $k \in \langle y \rangle \Rightarrow k = h \circ y$ for some $h \in G$.

$$\Rightarrow g \circ x = h \circ y$$
$$\Rightarrow x = g^{-1}h \circ y \quad \text{and} \quad y = h^{-1}g \circ x.$$

Take any element $\gamma \circ x \in \langle x \rangle$ for some $\gamma \in G$, observe that:

$$\gamma \circ x = \gamma g^{-1} h \circ y$$

Since $\gamma g^{-1} h \in G$.

$$\Rightarrow \gamma \circ x \in \langle y \rangle$$

$$\Rightarrow \langle x \rangle \subset \langle y \rangle.$$

Take any element $\beta \circ y \in \langle y \rangle$ for some $\beta \in G$, observe that

$$\beta \circ y = \beta h^{-1} g \circ y$$

Since $\beta h^{-1} g \in G$.

$\Rightarrow \beta \circ y \in \langle x \rangle$

$\Rightarrow \langle y \rangle \subset \langle x \rangle$.

Hence if $\langle x \rangle \wedge \langle y \rangle = \phi$

$\Rightarrow \langle x \rangle < \langle y \rangle \subset \langle x \rangle$

$\Rightarrow \langle x \rangle = \langle y \rangle$.

Hence it suffices to take $x_1, \ldots, x_m$ in the set X representing the distinct orbits; the set-theoretic class equation is:

$$X = \coprod_{i=1}^{m} \langle x_i \rangle .$$

Taking the cardinals, the numerical form of the class equation is:

$$|X| = \sum_{i=1}^{m} |\langle x_i \rangle|$$

Lets prove there exist a bijection between $\langle x \rangle \leftrightarrow G/G_x$, where $G/G_x = \{ gG_x : g \in G \}$

Define the mapping:

$$\psi : G/G_x \to \langle x \rangle .$$

$$\psi(gG_x) = g \circ x .$$

Lets show that ψ is well defined:

Take: $g_1 G_x = g_2 G_x$

$\Rightarrow g_2^{-1} g_1 \in G_x$

$\Rightarrow g_2^{-1} g_1 \circ x = x$

$\Rightarrow g_1 \circ x = g_2 \circ x.$

Hence ψ is well defined.

Lets show ψ is injective.

Take $\psi(g_1 G_x) = \psi(g_2 G_x)$

$\Rightarrow g_1 \circ x = g_2 \circ x$

$\Rightarrow g_2^{-1} g_1 \circ x = x$

$\Rightarrow g_2^{-1} g_1 \in G_x$

$\Rightarrow g_1 G_x = g_2 G_x.$

Hence ψ is injective.

Lets show ψ is surjective.

For any element in $\langle x \rangle$ will have the form $g \circ x$ for some $g \in G$.

Using that $g \in G$, there clearly exist $g G_x$ st

$$\psi(g G_x) = g \circ x.$$

Hence ψ is surjective.

Hence ψ is a bijective mapping.

Hence it suffices to say:

$$|\langle x_i \rangle| = |G| / |G_{x_i}|$$

Hence the numerical class equation becomes

$$|X| = \sum_{i=1}^{m} |G| / |G_{x_i}|$$

where $x_1, \ldots, x_m$ is the set of coset representatives.

—/—

c, ci) $\circ : D_{14} \times D_{14} \longrightarrow D_{14}$; $g \circ h = ghg^{-1}$.

$D_{14} = \langle x, y \mid x^7 = 1, y^2 = 1, yx = x^6 y \rangle$

$D_{14} = \{1, x, x^2, x^3, x^4, x^5, x^6, y, xy, x^2y, x^3y, x^4y, x^5y, x^6y\}$.

Lets find the disnict orbitals and the stability group.

Lets find $\langle 1 \rangle$

$\forall g \in D_{14}$, $g \circ 1 = g1g^{-1} = 1$

$\Rightarrow \langle 1 \rangle = \{1\}$, $G_1 = D_{14}$.

Lets find $\langle x \rangle$

$$1 \circ x = 1 x 1 = x.$$

$$x^a \circ x = (x^a) x (x^a)^{-1}$$

Obviously $x^a \circ x = x \quad \forall a = 1, \ldots, 6$

$$y \circ x = yxy^{-1} = yxy = x^5 yy = x^6$$

$$(x^a y) \circ x = x^a y x y^{-1} (x^a)^{-1} = x^a y x y (x^a)^{-1} = x^a x^6 (x^a)^{-1}$$

Obviously $(x^a y) \circ x = x^6 \quad \forall a = 1, \ldots, 6$

$\Rightarrow \langle x \rangle = \{x, x^6\}, G_x = \{1, x, x^2, x^3, x^4, x^5, x^6\}$

Lets find $\langle x^2 \rangle$;

$$1 \circ x^2 = 1 x^2 = x^2$$

$$x^a \circ x^2 = (x^a) x^2 (x^a)^{-1}$$

Obviously $x^a \circ x = x^2 \quad \forall a = 1, \ldots, 6.$

$$y \circ x^2 = yx^2y^{-1} = yx^2y = x^6 yxy = x^5 y^2$$

$\ldots = x^5$

$$(x^a y) \circ x^2 = x^a y x^2 y^{-1} (x^a)^{-1}$$
$$= x^a x^5 (x^a)^{-1}$$

Obviously $(x^a y) \circ x^2 = x^5 \quad \forall a = 1, \ldots, 6.$

$\Rightarrow \langle x^2 \rangle = \{x^2, x^5\}, G_{x^2} = \{1, x, x^2, x^3, x^4, x^5, x^6\}.$

Lets find $\langle x^3 \rangle$

$$1 \circ x^3 = 1 x^3 1$$
$$= x^3$$

$$x^a \circ x^3 = x^a x^3 (x^a)^{-1}$$

Obviously $x^a \circ x^3 = x^3 \quad \forall a = 1, \ldots, 6$

$$y \circ x^3 = y x^3 y^{-1}$$
$$= y x^3 y$$
$$= x^6 y x^2 y$$
$$= x^5 y x y$$
$$= x^4 y^2$$
$$= x^4$$

$$(x^a y) \circ x^3 = x^a y x^3 y^{-1} (x^a)$$
$$= x^a y x^3 y x^a$$
$$= x^a x^4 x^a.$$

Obviously $(x^a y) \circ x^3 = x^4 \quad \forall a = 1, \ldots, 6$

$\Rightarrow \langle x^3 \rangle = \{x^3, x^4\}, G_{x^3} = \{1, x, x^2, x^3, x^4, x^5, x^6\}.$

Lets find $\langle y \rangle$

$$1 \circ y = 1\, y\, 1 = y$$

$$x \circ y = x\, y\, x^{-1} = x\, y\, x^{6} = x x^{6}\, y\, x^{5} = y x^{5} = x^{6}\, y\, x^{4} = x^{5}\, y\, x^{3} = x^{4}\, y\, x^{2} = x^{3}\, y\, x = x^{2} y$$

$$x^{2} \circ y = x^{2} y x^{5} = x\, y\, x^{4} = y x^{3} = x^{6}\, y\, x^{2} = x^{5}\, y\, x = x^{4} y$$

$$x^{3} \circ y = x^{3} y x^{4} = x^{3} x^{6}\, y\, x^{3} = x^{2} y x^{3} = x\, y\, x^{2} = y x = x^{6} y$$

$$x^{4} \circ y = x^{4} y x^{3} = x^{4} x^{6}\, y\, x^{2} = x^{3} y\, x^{2} = x^{2} y x .$$

$\ldots = xy$

$$x^5 \circ y = x^5 y x^2$$
$$= x^5 x^6 y x$$
$$= x^4 y x$$
$$= x^3 y$$

$$x^6 \circ y = x^6 y x$$
$$= x^6 x^6 y$$
$$= x^5 y.$$

$$y \circ y = y y y^{-1}$$
$$= y y y$$
$$= y$$

$$(x^a y) \circ y = x^a y y y^{-1} (x^a)^{-1}$$
$$= x^a y (x^a)^{-1}$$

Hence
$$xy \circ y = x^2 y$$
$$x^2 y \circ y = x^4 y$$
$$x^3 y \circ y = x^6 y$$
$$x^4 y \circ y = xy$$
$$x^5 y \circ y = x^3 y$$
$$x^6 y \circ y = x^5 y$$

$\Rightarrow \langle y \rangle = \{y, xy, x^2 y, x^3 y, x^4 y, x^5 y, x^6 y\}$, $G_y = \{1, y\}$.

iii) Recall:

$\langle 1 \rangle = \{1\}$

$\langle x \rangle = \{x, x^6\}$

$\langle x^2 \rangle = \{x^2, x^5\}$

$\langle x^3 \rangle = \{x^3, x^4\}$

$\langle y \rangle = \{y, xy, x^2 y, x^3 y, x^4 y, x^5 y, x^6 y\}$

$G_1 = D_{14}$

$G_x = \{1, x, x^2, x^3, x^4, x^5, x^6\}$

$G_{x^2} = \{1, x, x^2, x^3, x^4, x^5, x^6\}$

$G_{x^3} = \{1, x, x^2, x^3, x^4, x^5, x^6\}$

$G_y = \{1, y\}$.

The set-theoretic class equation:

$$D_{14} = \langle 1 \rangle \amalg \langle x \rangle \amalg \langle x^2 \rangle \amalg \langle x^3 \rangle \amalg \langle y \rangle$$

$$= \{1\} \amalg \{x, x^6\} \amalg \{x^2, x^5\} \amalg \{x^3, x^4\} \amalg \{y, xy, x^2y, x^3y, x^4y, x^5y, x^6y\}.$$

The numerical class equation:

$$|D_{14}| = |\langle 1 \rangle| + |\langle x \rangle| + |\langle x^2 \rangle| + |\langle x^3 \rangle| + |\langle y \rangle|$$

$$= 1 + 2 + 2 + 2 + 7.$$

Using the other form of the numerical class equation:

$$|D_{14}| = |D_{14}|/|G_1| + |D_{14}|/|G_x| + |D_{14}|/|G_{x^2}| + |D_{14}|/|G_{x^3}| + |D_{14}|/|G_y|$$

$$= 14/14 + 14/7 + 14/7 + 14/7 + 14/2$$

—/—

3) Ansatz 1: Suppose K is a subgroup of the group G and $K \lhd G$ then product:

$$* : G/K \times G/K \longrightarrow G/K$$

$$(gK) * (hK) = (gh)K.$$

is well defined and a group product on G/K.

Ansatz 2: Suppose K, Q are a subgroup of the group G, if Q normalises K then

$$KQ = \{ kq : k \in K, q \in Q \}$$

is a subgroup of G and $K \lhd KQ$.

Ansatz 3: Noether's 0^{th} Isomorphism Theorem; Suppose G, H are groups and $\alpha : G \longrightarrow H$ is a group homomorphism then

$$G/Ker(\alpha) \cong Im(\alpha)$$

Lets show that $K \lhd G$ where $K = Ker(\alpha)$, assuming K is a subgroup of G it suffices to show $gkg^{-1} \in K$ $\forall g \in G$, $\forall k \in K$.

Take $\alpha(gkg^{-1})$

$= \alpha(gk)\alpha(g^{-1})$

$= \alpha(g)\alpha(k)\alpha(g^{-1})$

$= \alpha(g)\alpha(g^{-1})$ since $\alpha(k) = 1$ $\forall k \in K$

$= \alpha(gg^{-1})$

$= \alpha(1)$

$= 1$ $\forall k \in K$, $\forall g \in G$.

Hence $gkg^{-1} \in K \quad \forall g \in G, \forall k \in K$. Hence K is true. Hence G/K is a group under the product

Lets show the hypothesis, define the mapping:

$$\psi : G/K \longrightarrow Im(\alpha).$$

$$\psi(gK) = \alpha(g).$$

Assuming ψ is a well defined bijective mapping it suffices to show ψ is a homomorphism:

Take $\psi((g_1K)*(g_2K))$

$$= \psi((g_1g_2)K)$$

$$= \alpha(g_1g_2)$$

$$= \alpha(g_1)\alpha(g_2)$$

$$= \psi(g_1K)\psi(gK)$$

Hence ψ is a homomorphism, hence ψ is a isomorphism i.e $G/Ker(\alpha) \cong Im(\alpha)$

P, Q subgroups, G group.

P normalizes Q means $\forall p \in P, \forall q \in Q$ $pqp^{-1} \in Q$.

To prove $PQ/Q \cong P/(P \cap Q)$ when P normalizes Q, define the mapping:

$$\mathcal{V}: P \longrightarrow PQ/Q.$$

$$\mathcal{V}(p) = pQ.$$

where $PQ/Q = \{ hQ : h \in PH \}$

Lets show $\mathcal{V}$ is a homomorphism:

Take : $\mathcal{V}(p_1 p_2)$

$= (p_1 p_2)Q$

$= (p_1 Q) * (p_2 Q)$

$= \mathcal{V}(p_1)\mathcal{V}(p_2) \quad \forall p_1, p_2 \in P$

Hence $\mathcal{V}$ is a homomorphism, hence

$$P/\mathrm{Ker}(\mathcal{V}) \cong \mathrm{Im}(\mathcal{V})$$

Lets show $\mathrm{Im}(\mathcal{V}) = PQ/Q$ i.e $\mathcal{V}$ is surjective.

Observe for any arbitrary element in PQ/Q is of the form pqQ for some $p \in P$ and $q \in Q$. Observe that $pqQ = pQ$ since Q is a subgroup hence it has closure. Hence taking the $p \in P$ it suffices to say $\mathcal{V}(p) = pQ$. So $\mathcal{V}$ is surjective.

Hence $\mathrm{Im}(\mathcal{V}) = PQ/Q$.

Lets show $\mathrm{Ker}(\mathcal{V}) = P \wedge Q$.

By definition:

$$\mathrm{Ker}(\nu) = \{ p \in P : \nu(p) = Q \}.$$

Note that Q is defined to be the identity of the group PQ/P.

Take $\nu(p) = Q$

$$\Rightarrow pQ = Q$$

$$\Rightarrow p \in Q$$

But $p \in P$ hence $p \in P \wedge Q$

$$\Rightarrow \mathrm{Ker}(\nu) = P \wedge Q.$$

Hence:

$$P/(P \wedge Q) \cong PQ/Q$$

is proven.

—/—

Ansatz: Let G be a group and X a set. By a left action of G in X means a mapping

$$* \; G \times X \longrightarrow X$$

$$*(g, x) = g * x$$

such that:

i) $\forall g, h \in G \;\; \forall x \in X \quad (gh) * x = g * h * x$

ii) $\forall x \in X \quad 1 \cdot x = x.$

Ansatz: If X is a set where $|X| = n$ and $k \geq 0$ an integer and

$$\tilde{X} = \{ A \subset X \ : |A| = k \}.$$

Then: $|\tilde{X}| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$

To prove this hypothesis observe that the number of ordered k-tuple of distinct elements of X is $n(n-1)\dots(n-k+1)$.

Each k-subset of X occurs $k!$ times

$\Rightarrow$ The number of k subsets for X is

$$\frac{n(n-1)\dots(n-k+1)}{k!} = \binom{n}{k}$$

$$\Rightarrow |\tilde{X}| = \binom{n}{k}$$

Wilson's theorem: Let p be a prime and $k \geq 0$ integer. Then

$$\binom{kp^n}{p^n} = k \pmod{p}.$$

Proof: Let P be a group st $|P| = p^n$.

Define the set X as $X = P \times \{1, \dots, k\}$ hence $|X| = kp^n$.

Define the left action of the group P acting on X as:

$$\cdot : P \times X \to X$$

$$g \cdot (h, i) = (gh, i).$$

Define the set S' as $S' = \{A \subset X : |A| = p^n\}$.
By the ansatz:

$$|S'| = \binom{kp^n}{p^n}$$

Define the left action of the group P action on S' as

$$* : P \times S' \to S'$$

$$g * A = gA$$

where $gA = \{ga : a \in A\}$.

Since $|P| = p^n$ and $*$ is a left action of the group P on S' then:

$$|S'| = |S'^P| \pmod p$$

where $|S'^P| = \{A \in S' : \forall g \in P \quad g * A = A\}$.

$$\Rightarrow \binom{kp^n}{p^n} = |S'^P| \pmod p.$$

Lets show $|S'^P| = k$

Hence lets show for all $H \in S^P$, $H = P \times \{r\}$ for some $r \in \{1, \ldots, k\}$.

Hence lets show $P \times \{r\} \subset H$. For any arbitrary element $a \in P \times \{r\}$ will have the form $a = (h, r)$ for some $h \in P$

Take $g \cdot (h, r) = (gh, r)$

Since $gh \in P$ for any $g \in P \Rightarrow (gh, r) \in H$ hence $P \times \{r\} \subset H$. Since $|P \times \{r\}| = |H| = p^n$

$\Rightarrow P \times \{r\} = H$.

$\Rightarrow P \times \{r\} \in S^P \quad \forall r \in \{1, \ldots, k\}$.

Since $r = 1, \ldots, k$

$\Rightarrow |S^P| = k$

$\Rightarrow \binom{kp^n}{p^n} = k \pmod p$.

—/—

See paper guide for 2012, question 3, part 2 of 3.

—/—

Erratum: Question 4 part 1 of 2 is missing the following ansatzes:

Ansatz 1: Let K a group. $Aut(K)$ is a group under the product:

$$\circ : Aut(K) \times Aut(K) \to Aut(K).$$

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)) \quad \forall x \in K.$$

Ansatz 2: Let Q and K be subgroups of the group G and $h : Q \to Aut(K)$ is a homomorphism $K \rtimes_h Q$ is a group under the product:

$$* : (K \rtimes_h Q) \times (K \rtimes_h Q) \to (K \rtimes_h Q)$$

$$(k_1, q_1) * (k_2, q_2) = (k_1 h(q_1)(k_2), q_1 q_2).$$

4) K, Q subgroups, G group.

Lets show that $K \cap Q = \{1\}$. By contradiction suppose $K \cap Q \neq \{1\}$ i.e $\exists k \neq 1$ st $k \in K \cap Q$.
$\Rightarrow$ By Langranage $ord(k) \mid |K|$ and $ord(k) \mid |Q|$.
$\Rightarrow HCF(|K|, |Q|) = ord(k) > 1$. This is a contradiction since $(|K|, |Q|) = 1$. Hence $K \cap Q = \{1\}$ is true.

Lets define $K \rtimes_h Q$, for some homomorphism $h : Q \to Aut(K)$.

Define the mapping

$$h : Q \to Aut(K)$$
$$h(q)(k) = qkq^{-1}$$

$h(q)$ is a well defined mapping since $K \trianglelefteq G$, lets show h is a homomorphism:

Take $h(q_1 q_2)(k) = (q_1 q_2)(k)(q_1 q_2)^{-1}$

$$= q_1 q_2 k q_2^{-1} q_1$$
$$= h(q_1)(q_2 k q_2^{-1})$$
$$= h(q_1)(h(q_2)(k))$$
$$= h(q_1) \circ h(q_2)(k).$$

$$\Rightarrow h(q_1 q_2)(k) = h(q_1) \circ h(q_2).$$

Hence h is a homomorphism.

Hence $K \rtimes_h Q$ for some homomorphism $h: Q \to Aut(K)$ is defined.

Lets prove $G \cong K \rtimes_h Q$, define the mapping

$$\Phi : K \rtimes_h Q \longrightarrow G.$$

$$\Phi(k, q) = kq.$$

Lets show Φ is a homomorphism:

Take: $\Phi((k_1, q_1) * (k_2, q_2)) = \Phi(k_1 h(q_1)(k_2), q_1 q_2)$

$= \Phi(k_1 q_1 k_2 q_1^{-1}, q_1 q_2)$

$= k_1 q_1 k_2 q_1^{-1} q_1 q_2$

$= k_1 q_1 k_2 q_2$

$= \Phi(k_1, q_1)\Phi(k_2, q_2)$

Hence Φ is a homomiorphism

Lets show Φ is injective:

Take: $\Phi(k_1, q_1) = \Phi(k_2, q_2)$

$\Rightarrow k_1 q_1 = k_2 q_2$

$\Rightarrow k_2^{-1} k_1 = q_2 q_1^{-1}$

Obviously $k_2^{-1} k_1 \in K$ and $q_2 q_1^{-1} \in Q$ but $k_2^{-1} k_1 = q_1 q_2^{-1}$

Hence $q_2 q_1^{-1} \in K$ and $k_2^{-1} k_1 \in Q$ but $K \cap Q = 1$

$\Rightarrow q_2 q_1^{-1} = 1$ and $k_2^{-1} k_1 = 1$.

$\Rightarrow q_1 = q_2$ and $k_1 = k_2$.

Hence Φ is injective.

Lets show Φ is surjective.

Since $K \rtimes_h Q$ is defined as the set $K \times Q$.

$\Rightarrow |K \rtimes_h Q| = |K \times Q| = |K||Q|$

Since Φ is an injective homomorphism between two finite sets of the same cardinal, $|K||Q| = |G|$. Hence Φ is surjective.

Hence Φ is an isomorphism i.e $G \cong K \rtimes_h Q$ for some homomorphism $h : Q \to Aut(K)$.

—/—

Ansatz: Suppose that Q is subgroup of the group G then gQg^{-1} is also a subgroup of G, $\forall g \in G$ and $|gQg^{-1}| = |Q|$.

Lets state Sylow's theorem: Suppose p is prime and G is a finite group with $|G| = kp^n$ where $p \nmid k$ then:

i) G has at least one subgroup of order p^n.
ii) If N_p be the number of subgroups of G of order p^n. Then $N_p \equiv 1 \pmod p$.

Lets show G has a normal subgroup of order 29.

Observe $|G| = 725 = 5^2 \times 29$, 5 and 29 are prime and $5^2 \nmid 29$.

By Sylow's theorem $\exists K_7$ subgroup of G st $|K_7| = 29$. Since 29 is prime, $K_7 \cong C_{29}$.

By Sylow's theorem:

$$N_{29} \equiv 1 \pmod{29}.$$

Lets prove that $N_{29} = 1$, by contradiction suppose $N_{29} \neq 1 \Rightarrow N_{29} \geq 30$ i.e there exist at least $K_{7_1}, \ldots, K_{7_{30}}$ distinct subgroups of order 29. Since 29 is prime $K_{7_i} \cong C_{29}$ for each i.

Lets prove that $K_{7_i} \cap K_{7_j} = \{1\}$ $\forall i \neq j$. By contradiction suppose that $K_{7_i} \cap K_{7_j} \neq \{1\}$ i.e $\exists k \neq 1$ st $k \in K_{7_i} \cap K_{7_j}$. Hence $\text{ord}(k) = 29 \Rightarrow k$ will generate both K_{7_i} and $K_{7_j} \Rightarrow K_{7_i} = K_{7_j}$. This is a contradiction as K_{7_i} and K_{7_j} are distinct subgroups. Hence $K_{7_i} \cap K_{7_j} = \{1\}$ is true.

Hence there exist at least $30 \times (29-1) = 840$ elements in G but $|G| = 729 \not\geq 840$ hence contradiction. Hence $N_{29} = 1$ is true.

Since $N_{29} = 1 \Rightarrow K_7 \cong C_{29}$ is a unique subgroup of order 29

Since gK_7g^{-1} is also a subgroup of order 29

hence by uniqueness:

$$gKg^{-1} = K \qquad \forall g \in G.$$

$$\Rightarrow K \trianglelefteq G.$$

G has a has a normal subgroup of order 29.

Lets classify all groups of order 725.

By Sylow's theorem $\exists$ Q subgroup of G st $|Q| = 25$.

Since K, Q are groups of G where $(|K|, |Q|) = 1$ i.e K, Q are of coprime order and $K \trianglelefteq G$ and $|G| = |K||Q|$. By the previous hypothesis $G \cong K \rtimes_h Q$ for some homomorphism $h: Q \to Aut(K)$.

Since $K \cong C_{29}$ and $|Q| = 25 \Rightarrow$ either $Q \cong C_{25}$ or $Q \cong C_5 \times C_5$. Hence consider the cases:

i) $G \cong C_{29} \rtimes_h C_{25}$

ii) $G \cong C_{29} \rtimes_h (C_5 \times C_5)$.

where:

$$C_{29} = \langle a \mid a^{29} = 1 \rangle$$

$$C_{25} = \langle b \mid b^{25} = 1 \rangle$$

$$C_5 \times C_5 = \langle c, d \mid c^5 = d^5 = 1, \ cd = dc \rangle.$$

Case 1: $G \cong C_{29} \rtimes_h C_{25}$, for some homomorphism $h: C_{25} \to Aut(C_{29})$.

Lets find all homomorphisms $h: C_{25} \to Aut(C_{29})$, Since 29 is prime $\Rightarrow Aut(C_{29}) \cong C_{28}$ and

$(25, 28) = 1$ hence it suffices to say that the only homomorphism is $h_0(b) = \phi_1$ (i.e the trival homomorphism)

Lets do the critical calculation for $C_{29} \rtimes_{h_0} C_{25}$; $h_0 : C_{25} \to Aut(C_{29})$.

Take: $B = (1, b)$, $A = (a, 1)$.

$$\begin{aligned} B * A &= (1, b) * (a, 1) \\ &= (h_0(b)(a), b) \\ &= (\phi_1(a), b) \\ &= (a, b) \\ &= A * B. \end{aligned}$$

Hence:
$C_{29} \rtimes_h C_{25} = \langle A, B \mid A^{29} = B^{25} = 1, BA = AB \rangle$

Case 2: $G \cong C_{29} \rtimes_h (C_5 \times C_5)$, for some homomorphism $h : C_5 \times C_5 \to Aut(C_{29})$.

Let find all homomorphism $h : C_5 \times C_5 \to Aut(C_{29})$
Since 29 is prime $\Rightarrow Aut(C_{29}) \cong C_{28}$ and $(5, 28) = 1$ hence it suffices to say that the only homomorphism is $h_0(c) = \phi_1$, $h_0(d) = \phi_1$ (i.e the trival homomorphism).

Lets do the critical calculation for $C_{29} \rtimes_{h_0} (C_5 \times C_5)$; $h_0 : C_5 \times C_5 \to Aut(C_{29})$.

Take $C = (1, c)$, $D = (1, d)$, $A = (a, 1)$

$$C * A = (1, c) * (a, 1)$$

$$\begin{aligned} \ldots &= (h_0(c)(a), c) \\ &= (\phi_1(a), c) \\ &= (a, c) \\ &= A * C. \end{aligned}$$

$$\begin{aligned} D * A &= (1, d) * (a, 1) \\ &= (h_0(d)(a), d) \\ &= (\phi_1(a), d) \\ &= (a, d) \\ &= A * D \end{aligned}$$

Hence

$$C_{29} \rtimes_h (C_5 \times C_5) = \langle A, C, D \mid A^{29} = C^5 = D^5, CD = DC, CA = AC, DA = AD \rangle$$

Hence there are two distinct groups of order 729 either:

$$G \cong \langle A, B \mid A^{29} = B^{25} = 1, BA = AB \rangle$$

or

$$G \cong \langle A, C, D \mid A^{29} = C^5 = D^5, CD = DC, CA = AC, DA = AD \rangle$$

—/—

5) See paper guide for 2012, question 5, part 1 of 4.

—/—

Ansatz: Suppose that $\deg p(x) = 2$ then $p(x)$ is irreducible over $\mathbb{F} \iff \forall a \in \mathbb{F}, p(a) \neq 0$

Let $p(x) = x^2 + x + 2$,

$$\begin{aligned} p(0) &= 2 \not\equiv 0 \pmod 5 \\ p(1) &= 4 \not\equiv 0 \pmod 5 \\ p(2) &= 3 \not\equiv 0 \pmod 5 \\ p(3) &= 4 \not\equiv 0 \pmod 5 \\ p(4) &= 2 \not\equiv 0 \pmod 5 \end{aligned}$$

Hence $p(x) = x^2 + x + 2$ is irreducible over $\mathbb{F}_5$.

Let $p(x) = x^2 + 2x + 3$

$$\begin{aligned} p(0) &= 3 \not\equiv 0 \pmod 5 \\ p(1) &= 1 \not\equiv 0 \pmod 5 \\ p(2) &= -1 \not\equiv 0 \pmod 5 \\ p(3) &= 3 \not\equiv 0 \pmod 5 \\ p(4) &= 2 \not\equiv 0 \pmod 5 \end{aligned}$$

—/—

$f : \mathbb{F}_5[x]/(x^2+x+2) \to \mathbb{F}_5[x]/(x^2+2x+3)$

Observe that $x^2 + x + 2 \equiv 0$ in $\mathbb{F}_5[x]/(x^2+x+2)$

Observe that when $x \mapsto -2x$ then

$$x^2 + x + 2 \mapsto (-2x^2) + (-2x) + 2.$$

$$\ldots = 4x^2 + 3x + 2$$
$$= -y^2 - 2x - 3$$
$$= -(y^2 + 2x + 3)$$

Hence $x^2 + x + 2 \to 0$ in $\mathbb{F}_5[x]/(x^2+2x+3)$.

Using the observation, define the mapping:

$$\varphi : \mathbb{F}_5[x]/(x^2+x+2) \to \mathbb{F}_5[x]/(x^2+2x+3)$$

$$\varphi(ax+b) = -2ax+b.$$

Lets show that there is a ring homomorphism:

For addition; take:

$$\varphi((a_1x+b_1) + (a_2x+b_2))$$
$$= \varphi((a_1+a_2)x + (b_1+b_2))$$
$$= -2(a_1+a_2)x + (b_1+b_2)$$
$$= (-2a_1x+b_1) + (-2a_2x+b_2)$$
$$= \varphi(a_1x+b_1) + \varphi(a_2x+b_2)$$

Hence: $\varphi((a_1x+b_1) + (a_2x+b_2)) = \varphi(a_1x+b_1) + \varphi(a_2x+b_2)$

For multiplication; take:

$$\varphi(a_1x+b)\,\varphi(a_2x+b_2)$$
$$= (-2a_1x+b)(-2a_2x+b_2)$$
$$= 4a_1a_2x^2 - 2a_1b_2x - 2a_2b_1x + b_1b_2$$

Since $x^2 = 3x+2$ in $\mathbb{F}_5[x]/(x^2+2x+3)$, hence:

$$\ldots = 4a_1a_2(3x+2) - 2a_1b_2x - 2a_2b_1x + b_1b_2$$

$$\ldots = 12a_1a_2x + 8a_1a_2 - 2a_1b_2x - 2a_2b_1x + b_1b_2$$
$$= 2a_1a_2x + 3a_1b_2x + 3a_2b_1x + b_1b_2 + 3a_1a_2.$$

Take: $\ell((a_1x+b_1)\cdot(a_2x+b_2))$
$= \ell(a_1a_2x^2 + a_1b_2x + a_2b_1x + b_1b_2)$

Since $x^2 = 4x+3$ in $\mathbb{F}_5[x]/(x^2+x+2)$ hence

$$\ldots = \ell(a_1a_2(4x+3) + a_1b_2x + a_2b_1x + b_1b_2)$$
$$= \ell((4a_1a_2 + a_1b_2 + a_2b_1)x + (3a_1a_2 + b_1b_2))$$
$$= -2(4a_1a_2 + a_1b_2 + a_2b_1)x + (3a_1a_2 + b_1b_2)$$
$$= -8a_1a_2x - 2a_1b_2x - 2a_2b_1x + 3a_1a_2 + b_1b_2$$
$$= 2a_1a_2x + 3a_1b_2x + 3a_2b_1x + b_1b_2 + 3a_1a_2$$

Hence: $\ell((a_1x+b_1)\cdot(a_2x+b_2)) = \ell(a_1x+b_1)\ell(a_2x+b_2)$

For identity; take:

$$\ell(1) = \ell(0x+1)$$
$$= -2(0) + 1$$
$$= 1.$$

Hence $\ell(1) = 1$.

Hence ℓ is a ring homomorphism.

Lets show ℓ is a bijective mapping, hence lets show ℓ is injective; take.

$$\ell(ax+b) = \ell(a'x+b')$$
$$\Rightarrow -2ax + b = -2a'x + b'$$
$$\Rightarrow -2ax + 2a'x + b - b' = 0$$
$$\Rightarrow (-2a + 2a')x + (b - b') = 0.$$

$\Rightarrow -2a + 2a' = 0$ and $b - b' = 0$

$\Rightarrow a = a'$ and $b = b'$.

$\Rightarrow ax + b = a'x + b'$

Hence ℓ is injective.

Let prove ℓ is surjective. Obviously;

$$|\mathbb{F}_5[x]/(x^2+x+2)| = |\mathbb{F}_5[x]/(x^2+2x+3)|$$

Hence ℓ is a mapping between two finite sets of the same cardinal and ℓ is injective $\Rightarrow \ell$ is surjective.

Hence ℓ is bijective ring homomorphism

Hence ℓ is a ring isomorphism.

—/—

Observe that $x^2 = 3x + 2$ in $\mathbb{F}_5[x]/(x^2+x+2)$

Take:

$$\begin{aligned} x^3 &= x(3x+2) \\ &= 3x^2 + 2x \\ &= 3(3x+2) + 2x \\ &= 9x + 6 + 2x \\ &= x + 1. \end{aligned}$$

$$\begin{aligned} x^6 &= x^3 \cdot x^3 \\ &= (x+1)(x+1) \\ &= x^2 + 2x + 1 \\ &= 3x + 2 + 2x + 1 \\ &= 3 \end{aligned}$$

Hence $x^6 = 3$ in $\mathbb{F}_5[x]/(x^2+2x+3)$.

Take:

$$x^{12} = (x^6)^2 = 3 \cdot 3 = 4$$

$$x^{18} = (x^6)^3 = 4 \cdot 3 = 2$$

$$x^{24} = (x^6)^4 = 2 \cdot 3 = 1$$

Since $|(\mathbb{F}_5[x]/(x^2+2x+3))^*| = |(\mathbb{F}_5[x]/(x^2+2x+3)) - \{0\}| = 24$. It suffices to say that x generates the group $(\mathbb{F}_5[x]/(x^2+2x+3))^*$

—/—

Since ℓ "preserves" the orders of each element, lets find a, b st $\ell(ax+b) = x$.

Take: $\ell(ax+b) = -2ax + b$

$\Rightarrow -2ax + b = x$

$\Rightarrow -2a = 1$ and $b = 0$.

Hence $a = 2$ since $-2 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$

Hence $2x$ is a generator for $(\mathbb{F}_5[x]/(x^2+x+2))^*$.

—/—

6) See paper guide for 2012, question 6, part of 5.

—/—

$a(x)$ has a proper factorization over $\mathbb{Z}$ when there is a factorisation:

$$a(x) = b(x)c(x)$$

where $b(x), c(x) \in \mathbb{Z}[x]$ and $\deg b(x) < \deg a(x)$ and $\deg c(x) < \deg a(x)$

—/—

Lets prove the hypothesis by contradiction suppose $a(x)$ is not irreducible over $\mathbb{Q}$ i.e

$$a(x) = \beta(x)\gamma(x)$$

for some $\beta(x), \gamma \in \mathbb{Q}[x]$ where $\beta(x), \gamma(x)$ are both non constants and $\deg \beta(x) < \deg a(x)$ $\deg \gamma(x) < \deg a(x)$.

Define:

$M :=$ The lowest common multiple denominators of coefficients of $\beta(x)$

$N :=$ The lowest common multiple denominators of coefficients of $\gamma(x)$.

Hence $M\beta(x) \in \mathbb{Z}[x]$, $N\gamma(x) \in \mathbb{Z}[x]$.

So: $MNa(x) = (M\beta(x))(N\gamma(x))$

Put: $b(x) = M\beta(x)$, $c(x) = N\gamma(x)$.

So: $\deg b(x) = \deg \beta(x) < \deg a(x)$
$\deg c(x) = \deg \gamma(x) < \deg a(x)$

Also $b(x), c(x) \in \mathbb{Z}[x]$.

Lets define:

$$A = C(a)$$
$$B = C(b)$$
$$C = C(c)$$

and define:

$$a(x) = A\, a_0(x) \quad , \quad a_0(x) \in \mathbb{Z}[x]$$
$$b(x) = B\, b_0(x) \quad , \quad b_0(x) \in \mathbb{Z}[x]$$
$$c(x) = C\, c_0(x) \quad , \quad c_0(x) \in \mathbb{Z}[x]$$

where $C(a_0) = C(b_0) = C(c_0) = 1$

Observe that:

$$\deg a_0(x) = \deg a(x)$$
$$\deg b_0(x) = \deg b(x) = \deg \beta(x)$$
$$\deg c_0(x) = \deg c(x) = \deg \gamma(x).$$

Hence: $MNa(x) = (M\beta(x))(N\gamma(x))$ becomes

$$MNAa_0(x) = BC\, b_0(x) c_0(x).$$

Lets find the content of $MNAa_0(x)$ i.e $C(MNAa_0(x))$. Since $C(a_0) = 1$, it suffices to say $C(MNAa_0(x)) = MNA$.

Let find the content of $BCb_0(x)c_0(x)$ i.e $C(BCb_0(x)c_0(x))$. Since $C(b_0) = C(c_0) = 1$, by Gauss' lemma $C(b_0c_0) = 1$, it suffices to say $C(BCb_0(x)c_0(x)) = BC$.

Obviously:

$$C(MNAa_0(x)) = C(BCb_0(x)c_0(x))$$
$$\Rightarrow \quad MNA = BC$$

Hence $MNAa_0(x) = BCb_0(x)c_0(x)$
$$\Rightarrow a_0(x) = b_0(x)c_0(x).$$

Multiply both sides by A

$$Aa_0(x) = Ab_0(x)c_0(x)$$
$$\Rightarrow a(x) = Ab_0(x)c_0(x).$$

where $\deg Ab_0(x) < \deg a(x)$, $\deg c_0(x) < \deg a(x)$ and $Ab_0(x) \in \mathbb{Z}[x]$, $c_0(x) \in \mathbb{Z}[x]$

$\Rightarrow a(x)$ has a proper factorisation over $\mathbb{Z}$.

This is a contradiction form the hypothesis, hence $a(x)$ is irreducible over $\mathbb{Q}$.

—/—

Ansatz: Assume here that:
i) Each $c_d(x) \in \mathbb{Z}[x]$ integral polynomial.

ii) Each $C_d(x)$ is **irreducible** over $\mathbb{Q}$.
iii) Each $C_d(x)$ is finite computable.
iv) $x^n - 1 = \prod_{d|n} C_d(x)$ for each n.

i) Observe that:
$(x+1)^5 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$

Hence:
$x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 12 = (x+1)^5 + 11.$

Take the substitution $x+1 \longmapsto x$, the polynomial becomes $x^5 + 11$

Observe that in $x^5 + 11$; $a_0 \not\equiv 0 \pmod{11^2}$, $a_r \equiv 0 \pmod{11}$ when $0 \leq r \leq 4$ and $a_5 \not\equiv 0 \pmod{11}$ and 11 is prime. Hence by Eisentsein's Criterion $x^5 + 11$ is irreducible over $\mathbb{Q}$.

Hence $x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 12$ is irreducible over $\mathbb{Q}$.

ii) $x^{12} + 2x^6 + 1$.

Observe that:
$x^{12} + 2x^6 + 1 = (x^6 + 1)(x^6 + 1)$.

Lets find all the irreducible factors of $x^6 + 1$.

Take: $x^{12} - 1 = (x^6 - 1)(x^6 + 1)$

$$\Rightarrow x^6 + 1 = \frac{x^{12} - 1}{x^6 - 1}$$

$$\Rightarrow x^6+1 = \frac{\prod_{d|12} C_d(x)}{\prod_{d|6} C_d(x)}$$

$$= \frac{C_1(x)C_2(x)C_3(x)C_4(x)C_6(x)C_{12}(x)}{C_1(x)C_2(x)C_3(x)C_{12}(x)}$$

$$= C_4(x)C_{12}(x).$$

Lets find $C_4(x)$,

$$x^4-1 = \prod_{d|4} C_d(x)$$

$$= C_1(x)C_2(x)C_4(x)$$

$$= (x^2-1)C_4(x)$$

$$\Rightarrow C_4(x) = \frac{x^4-1}{x^2-1} = x^2+1$$

lets find $C_{12}(x)$

$$x^{12}-1 = \prod_{d|12} C_d(x)$$

$$= C_1(x)C_2(x)C_3(x)C_4(x)C_6(x)C_{12}(x)$$

$$= (x^6-1)C_4(x)C_{12}(x).$$

$$\Rightarrow C_{12}(x)C_4(x) = x^6+1.$$

$$\Rightarrow C_{12}(x) = \frac{x^6+1}{x^2+1}$$

$$\Rightarrow C_{12}(x) = x^4-x^2+1.$$

The polynomial $x^{12} + 2x^6 + 1$ is not irreducible and its complete factorisation over $\mathbb{Q}$ is:

$$x^{12} + 2x^6 + 1 = (x^2+1)(x^2+1)(x^4-x^2+1)(x^4-x^2+1)$$

— / —