Uppsala Universitet
Matematiska Institutionen
Laertis Vaso

Algebraiska strukturer
Kandidatprogrammet i matematik
HT 2018

Exam in Algebraic Structures
08-01-2019

Time: 08.00-13.00. No notes, books or electronic devices allowed. Please write your answers in English or in Swedish. Justify all of your answers! Each problem gives 5 points. To get a grade of 3 you need at least 18 points, to get a grade of 4 you need at least 25 points and to get a grade of 5 you need at least 32 points.

1. (a) Let G be a group and $H \subset G$ be a subset of G. Show that H is a subgroup of G if and only if $H \neq \varnothing$ and for all $x, y \in H$ we have $xy^{-1} \in H$.

   (b) Let G be the set of all invertible complex 2×2-matrices. Then G is a group under usual matrix multiplication. Let
$$H = \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \mid w, z \in \mathbb{C}, (w, z) \neq (0, 0) \right\}.$$
   Is H a subgroup of G? *(Hint: recall that the inverse of an invertible complex 2×2-matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.)*

2. (a) Classify all abelian groups of order 900.

   (b) Classify all groups of order 961.

3. Let G be a group of order 45. Determine which of the following statements are true.

   (a) G has an element of order 9.

   (b) G has a subgroup of order 9.

   (c) G has a subgroup of order 5.

   (d) G has a normal subgroup of order 9.

   (e) G has a normal subgroup of order 5.

4. Let $\mathbb{R}^{2\times 2}$ be the set of all real 2×2-matrices. Then $\mathbb{R}^{2\times 2}$ is a ring under usual matrix addition and multiplication. For each of the following subsets of $\mathbb{R}^{2\times 2}$, decide whether it is a subring.

   (a) The set $T = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$.

   (b) The set $S = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$.

   (c) The set $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$.

TURN THE PAGE!

5. Let $q(X, Y) = X^2 + Y^2 - 1 \in \mathbb{C}[X, Y]$.
   (a) Show that $q(X, Y)$ is irreducible in $\mathbb{C}[X, Y]$.
   (b) Is $q(X, Y)$ prime?
   (c) Is $\mathbb{C}[X, Y]/(q(X, Y))$ a domain?

6. For each of the following field extensions, compute its degree.
   (a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.
   (b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$.
   (c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

7. (a) Show that a field morphism is always injective.
   (b) Let $\mathbb{F}_n$ be a finite field with n elements. Show that $x^{n-1} = 1$ for all $x \in \mathbb{F}_n \setminus \{0\}$.
   (c) Conclude that there is no field morphism $\mathbb{F}_8 \to \mathbb{F}_{32}$.

8. Let $E = \mathbb{Q}(\zeta)$, where $\zeta = e^{\frac{2\pi}{7} i}$.
   (a) Determine the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.
   (b) Describe all subgroups of $\mathrm{Gal}(E/\mathbb{Q})$, ordered by inclusion and all intermediate fields $\mathbb{Q} \subset F \subset E$, ordered by inclusion.

GOOD LUCK!

Solutions

1. (a) Assume first that $H \subset G$ is a subgroup. Then (SG2) implies $e \in H$ and so $H \neq \varnothing$. Moreover, for any $x, y \in H$ we have by (SG3) that $y^{-1} \in H$ and then by (SG2) that $xy^{-1} \in G$ which proves the "only if" part.

   Assume now that $H \neq \varnothing$ and $x, y \in H$ implies $xy^{-1} \in H$. Since $H \neq \varnothing$, there exists some element $x \in H$. Then since $x, x \in H$ we have by assumption that $xx^{-1} = e \in H$ which proves (SG2). Then for any $x \in H$ we have $e, x \in H$ and so by assumption $ex^{-1} = x^{-1} \in H$, which proves (SG3). Finally, for any $x, y \in H$ we have that $x, y^{-1} \in H$ (since (SG3) is satisfied) and so by assumption $x\left(y^{-1}\right)^{-1} = xy \in H$, which proves (SG1) and completes the proof.

   (b) Let $x = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \in H$. Then

$$\det(x) = w\overline{w} - (-z)\overline{z} = |w|^2 + |z|^2 > 0$$

   and so $x \in G$. Hence $H \subset G$. Moreover, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -0 \\ \overline{0} & \overline{1} \end{pmatrix} \in H$$

   and so $H \neq \varnothing$. Finally, if $x = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix}, y = \begin{pmatrix} u & -v \\ \overline{v} & \overline{u} \end{pmatrix} \in H$, then

$$\begin{aligned} xy^{-1} &= \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \cdot \frac{1}{|u|^2 + |v|^2} \begin{pmatrix} \overline{u} & v \\ -\overline{v} & u \end{pmatrix} \\ &= \frac{1}{|u|^2 + |v|^2} \begin{pmatrix} w\overline{u} + z\overline{v} & wv - zu \\ \overline{zu} - \overline{wv} & \overline{z}v + \overline{w}u \end{pmatrix} \\ &= \begin{pmatrix} \frac{w\overline{u} + z\overline{v}}{|u|^2+|v|^2} & -\frac{zu - wv}{|u|^2+|v|^2} \\ \frac{\overline{zu - wv}}{|u|^2+|v|^2} & \frac{\overline{w\overline{u}+z\overline{v}}}{|u|^2+|v|^2} \end{pmatrix} \in H, \end{aligned}$$

   and so by part (a) we conclude that H is a subgroup of G.

2. (a) We have that $900 = 2^2 \cdot 3^2 \cdot 5^2$. Hence by the fundamental theorem for finitely generated abelian groups, the abelian groups of order 900 are classified by

$$\begin{array}{ll} \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}, & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}, \\ \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5, & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5, \\ \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, \\ \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5. \end{array}$$

   (b) Since $961 = 31^2$ is a prime squared, all groups of order 961 are abelian. Hence the groups of order 961 are classified by the fundamental theorem for finitely generated abelian groups to be $\mathbb{Z}_{961}$ and $\mathbb{Z}_{31} \times \mathbb{Z}_{31}$.

3. (a) This is not true in general. For example, $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ has no element of order 9.

   (b) This is true by the first Sylow theorem since $9 = 3^2 \mid 45$.

   (c) This is true by the first Sylow theorem since $5 \mid 45$.

(d) This is true. To see this, let s_3 be the number of Sylow 3-subgroups of G. Then by the second Sylow theorem we have

$$\left.\begin{array}{l} s_3 \equiv 1 \pmod 3 \\ s_3 \mid 45 \end{array}\right\} \implies \left.\begin{array}{l} s_3 \in \{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43\} \\ s_3 \in \{1,3,5,9,15,45\} \end{array}\right\} \implies s_3 = 1.$$

and hence there exists exactly one Sylow 3-subgroup of G. Let us call it S. Then since 9 is the heighest power of 3 that divides 45, we have $|S| = 9$. Since aSa^{-1} is also a subgroup of G with 9 elements for any $a \in G$, we have that $aSa^{-1} = S$ for all $a \in G$ and so $aS = Sa$ for all $a \in G$, hence S is normal.

(e) This is true. To see this, let s_5 be the number of Sylow 5-subgroups of G. Then by the second Sylow theorem we have

$$\left.\begin{array}{l} s_5 \equiv 1 \pmod 5 \\ s_5 \mid 45 \end{array}\right\} \implies \left.\begin{array}{l} s_5 \in \{1,6,11,16,21,26,31,36,41\} \\ s_5 \in \{1,3,5,9,15,45\} \end{array}\right\} \implies s_5 = 1.$$

and hence there exists exactly one Sylow 5-subgroup of G. Let us call it T. Then since 5 is the heighest power of 5 that divides 45, we have $|T| = 5$. Since aTa^{-1} is also a subgroup of G with 5 elements for any $a \in G$, we have that $aTa^{-1} = T$ for all $a \in G$ and so $aT = Ta$ for all $a \in G$, hence T is normal.

4. (a) The set T is a subring of $\mathbb{R}^{2\times 2}$. We check the axioms:

(SR1) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$.

(SR2) Let $x = \begin{pmatrix} x_1 & 0 \\ x_2 & x_3 \end{pmatrix}, y = \begin{pmatrix} y_1 & 0 \\ y_2 & y_3 \end{pmatrix} \in T$. Then $x - y = \begin{pmatrix} x_1 - y_1 & 0 \\ x_2 - y_2 & x_3 - y_3 \end{pmatrix} \in T$.

(SR3) Let $x = \begin{pmatrix} x_1 & 0 \\ x_2 & x_3 \end{pmatrix}, y = \begin{pmatrix} y_1 & 0 \\ y_2 & y_3 \end{pmatrix} \in T$. Then $xy = \begin{pmatrix} x_1 y_1 & 0 \\ x_2 y_1 + x_3 y_2 & x_3 y_3 \end{pmatrix} \in T$.

(b) The set S is not a subring of $\mathbb{R}^{2\times 2}$ because (SR3) fails. For example, for $x = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in S$ we have $xy = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix} \notin S$.

(c) The set H is not a subring of $\mathbb{R}^{2\times 2}$ because (SR1) fails, since $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin H$.

5. (a) We can write $\mathbb{C}[X,Y] = (\mathbb{C}[X])[Y] = R[Y]$ with $R = \mathbb{C}[X]$. Then we write

$$q(X,Y) = X^2 + Y^2 - 1 = r_0 + r_1 Y + r_2 Y^2$$

for some $r_0, r_1, r_2 \in R$. Solving this system we immediately find $r_0 = X^2 - 1$, $r_1 = 0$, $r_2 = 1$. Our aim is to apply Eisenstein's criterion. Since $\mathbb{C}$ is a field, we have that $R = \mathbb{C}[X]$ is a ufd by Gauss's theorem. Moreover, $f \in R[Y]$ is primitive since $r_2 = 1$. Next, we have that $X + 1 \in \operatorname{irr}(R)$ because $X + 1$ has degree 1. Then

$$\begin{cases} X + 1 \nmid 1 = r_2 \\ X + 1 \mid 0 = r_1 \\ X + 1 \mid X^2 - 1 = r_0 \quad \text{since } X^2 - 1 = (X+1)(X-1) \\ (X+1)^2 \nmid X^2 - 1 \end{cases}$$

where the last statement follows because $(X+1)^2 g(X) = X^2 - 1 \implies \deg(g) = 0$ and so $g = c \in \mathbb{C}$, hence

$$cX^2 + 2cX + c = X^2 - 1 \implies (c-1)X^2 + 2cX + (c+1) = 0.$$

From this we get

$$\left.\begin{aligned} c-1 &= 0 \\ 2c &= 0 \\ c+1 &= 0 \end{aligned}\right\} \implies \left.\begin{aligned} c &= 1 \\ 2 &= 0 \\ 1+1 &= 0 \end{aligned}\right\}$$

which is impossible. Hence we can apply Eisenstein's criterion and we have that $q(X,Y) \in \operatorname{irr}(R[Y]) = \operatorname{irr}(\mathbb{C}[X,Y])$.

(b) Since $\mathbb{C}$ is a ufd, it follows that $\mathbb{C}[X,Y]$ is also a ufd by Gauss's theorem. Since $q(X,Y) \in \mathbb{C}[X,Y]$ is irreducible by (a), it follows that it is also prime.

(c) $\mathbb{C}[X,Y]/(q(X,Y))$ is a domain. To see this we check the axioms:

(D1) Since $\mathbb{C}[X,Y]$ is commutative, it follows that $\mathbb{C}[X,Y]/(q(X,Y))$ is also commutative since multiplication is inherited from $\mathbb{C}[X,Y]$.

(D2) We have $1 \notin (q(X,Y))$ since we clearly cannot have $1 = (X^2+Y^2-1)f(X,Y)$ by checking degrees. Hence

$$1_{\mathbb{C}[X,Y]} = 1 + (q(X,Y)) \neq 0 + (q(X,Y)) = 0_{\mathbb{C}[X,Y]},$$

as required.

(D3) Let $\overline{f} = f + (q(X,Y)), \overline{g} = g + (q(X,Y)) \in \mathbb{C}[X,Y]$ with $\overline{f}\overline{g} = 0_{\mathbb{C}[X,Y]}$. Then

$$\begin{aligned} (f + (q(X,Y)))(g + (q(X,Y))) = 0 + (q(X,Y)) &\implies fg + (q(X,Y)) = 0 + (q(X,Y)) \\ &\implies fg \in (q(X,Y)) \\ &\implies q(X,Y) \mid fg \\ &\overset{q(X,Y)\text{ prime}}{\implies} q(X,Y) \mid f \text{ or } q(X,Y) \mid g \\ &\implies f \in (q(X,Y)) \text{ or } g \in (q(X,Y)) \\ &\implies \overline{f} = 0_{\mathbb{C}[X,Y]} \text{ or } \overline{g} = 0_{\mathbb{C}[X,Y]}. \end{aligned}$$

6. (a) We have $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = \deg \operatorname{irrpol}_{\mathbb{Q}}\left(\sqrt{2}\right) = \deg\left(X^2 - 2\right) = 2$. That X^2-2 is irreducible over $\mathbb{Q}$ follows since its roots are $-\sqrt{2}, \sqrt{2} \notin \mathbb{Q}$ and any factorization of X^2-2 into non-units would have a degree 1 polynomial appearing, and so one term of the form $X - r$ with r being one of the roots of X^2-2. Since it is monic and has $\sqrt{2}$ as a root, it follows that $\operatorname{irrpol}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$.

(b) We have $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = \deg \operatorname{irrpol}_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = \deg\left(X^3-2\right) = 3$. That X^3-2 is irreducible over $\mathbb{Q}$ follows since its roots are $\sqrt[3]{2}, e^{\frac{2\pi}{3}i}\sqrt[3]{2}, e^{\frac{4\pi}{3}i}\sqrt[3]{2} \notin \mathbb{Q}$ and any factorization of X^3-2 into non-units would have a degree 1 polynomial appearing, and so one term of the form $X-r$ with r being one of the roots of X^3-2. Since it is monic and has $\sqrt[3]{2}$ as a root, it follows that $\operatorname{irrpol}_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = X^3-2$.

(c) We first compute $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]$. To this end we claim $\operatorname{irrpol}_{\mathbb{Q}(\sqrt[3]{2})}\left(\sqrt{2}\right) = X^2-2$. Since $X^2 - 2 \in \mathbb{Q}\left(\sqrt[3]{2}\right)(X)$ is monic and has $\sqrt{2}$ as a root, it is enough to show that it is irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Indeed, assume to a contradiction that it is not irreducible. Then it splits over $\mathbb{Q}\left(\sqrt[3]{2}\right)$, since it can be written as a product of two polynomials of degree 1. In particular $X^2-2 = \left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right)$ in $\mathbb{Q}\left(\sqrt[3]{2}\right)(X)$ implies that $\sqrt{2} \in \mathbb{Q}\left(\sqrt[3]{2}\right)$. Hence $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$ and so

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] \implies 3 = \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \cdot 2,$$

which is a contradiction. Hence X^2-2 is indeed irreducible over $\mathbb{Q}\left(\sqrt[3]{2}\right)$ and so $\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]=\deg \operatorname{irrpol}_{\mathbb{Q}(\sqrt[3]{2})}\left(\sqrt{2}\right)=\deg\left(X^2-2\right)=2$. Combining everything together, we have

$$\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=2\cdot 3=6.$$

7. (a) Let K,E be fields and $\phi : K \to E$ be a field morphism. It is enough to show that $\ker\phi=\{0_K\}$. Assume to a contradiction that for some $x\in K\setminus\{0_K\}$ we have $\phi(x)=0_E$. Then since K is a field and $x\neq 0_K$, there exists $x^{-1}\in K$ with $1_K=x^{-1}x$. Moreover, since ϕ is a field morphism, we have $\phi(1_K)=1_E$. Then

$$1_E=\phi(1_K)=\phi(x^{-1}x)=\phi(x^{-1})\phi(x)=\phi(x^{-1})0_E=0_E,$$

and so $1_E=0_E$, contradicting the fact that E is a field. Hence $\ker\phi=\{0_K\}$ and ϕ is injective.

(b) Since $\mathbb{F}_n$ is a field, we have that $\mathbb{F}_n^\times=\mathbb{F}_n\setminus\{0\}$. In particular, the unit group $\mathbb{F}_n^\times$ has order $|\mathbb{F}_n^\times|=n-1$ and so for every $x\in\mathbb{F}_n^\times$ we have $x^{n-1}=1$ by Lagrange's theorem.

(c) Assume to a contradiction that there exists such a field morphism $g:\mathbb{F}_8\to\mathbb{F}_{32}$ and let $x\in\mathbb{F}_8\setminus\{0,1\}$. Then by (b) we have $x^7=1$ and so

$$g(x)^7=g(x^7)=g(1)=1,$$

since g is a field morphism. On the other hand, again by (b) we have $g(x)^{31}=1$. Then

$$\left.\begin{matrix} g(x)^7=1\\ g(x)^{31}=1\end{matrix}\right\}\implies\left.\begin{matrix} \mathrm{o}(g(x))\mid 7\\ \mathrm{o}(g(x))\mid 31\end{matrix}\right\}\implies \mathrm{o}(g(x))=1\implies g(x)^1=1\implies g(x)=1.$$

But we also have $g(1)=1$ and $x\neq 1$ by assumption. Hence g is not injective and we reach a contradiction by (a). Therefore such a field morphism does not exist.

8. (a) We know that $E=\mathrm{sf}(\Phi_7)$. Hence the field extension $\mathbb{Q}\subset E$ is algebraic and normal. Since $\mathrm{char}(\mathbb{Q})=0$, we have that $\mathbb{Q}\subset E$ is a separable field extension and so it is finite. Therefore, it is a finite Galois extension. We have seen for the polynomial $\Phi_7(X)\in\mathbb{Q}[X]$ that it is irreducible and separable, and its set of roots is

$$R=\{\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5,\zeta^6\}.$$

Hence every $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$ induces a permutation $\sigma_R:R\to R$, in other words $\sigma_R\in S_6$. It follows that the map $\rho:\mathrm{Gal}(E/\mathbb{Q})\to S_6$ defined by $\rho(\sigma)=\sigma_R$ is a monomorphism, and in particular we have that $\mathrm{Gal}(E/\mathbb{Q})\cong\operatorname{im}\rho<S_6$. Therefore, we need to describe $\operatorname{im}\rho$.

Let $\pi\in\operatorname{im}\rho$, that is $\pi=\sigma_R$ for some $\sigma\in\mathrm{Gal}(E/\mathbb{Q})$. Then

$$\pi(\zeta)=\zeta^h$$

for some $h\in\{1,2,3,4,5,6\}$. It follows that for every $i\in\{1,2,3,4,5,6\}$ we have

$$\pi(\zeta^i)=\sigma(\zeta^i)=\sigma(\zeta)^i=(\zeta^h)^i=\zeta^{hi}.$$

Hence to determine π, it is enough to determine h since then we have

$$\pi(\zeta^i)=\zeta^{hi},$$

for all $\zeta^i\in R$. Hence we can write $\pi=\pi_h$ with $\pi_h(\zeta^i)=\zeta^{hi}$. Therefore,

$$\operatorname{im}\rho\subset\{\pi_1,\pi_2,\pi_3,\pi_4,\pi_5,\pi_6\}.$$

We now want to show the other inclusion as well. That is, for each $h \in \{1,2,3,4,5,6\}$ we need to find a $\sigma \in \operatorname{Gal}(E/\mathbb{Q})$ such that $\sigma(\zeta) = \zeta^h$, since $\sigma(\zeta^i) = \zeta^{hi} = \pi_h(\zeta^i)$ implies $\rho(\sigma) = \sigma_R = \pi_h$ and so $\pi_h \in \operatorname{im}\rho$. We know that $\operatorname{irrpol}_{\mathbb{Q}}(\zeta) = \Phi_7(X)$ generates $\ker \epsilon_\zeta$. Similarly, $\operatorname{irrpol}_{\mathbb{Q}}(\zeta^h) = \Phi_7(X)$ and it generates $\ker \epsilon_{\zeta^h}$. In particular, we have isomorphisms

$$\overline{\epsilon}_\zeta : \mathbb{Q}[X]/\left(\Phi_7(X)\right) \xrightarrow{\sim} \mathbb{Q}(\zeta),$$
$$\overline{\epsilon}_{\zeta^h} : \mathbb{Q}[X]/\left(\Phi_7(X)\right) \xrightarrow{\sim} \mathbb{Q}(\zeta^h).$$

Hence the composition

$$\sigma := \overline{\epsilon}_{\zeta^h}\overline{\epsilon}_\zeta^{-1} : \mathbb{Q}(\zeta) \xrightarrow{\sim} \mathbb{Q}(\zeta^h)$$

is a field isomorphism and it satisfies $\sigma(\zeta) = \zeta^h$. Moreover, we have the field extensions

$$\mathbb{Q} \subset \mathbb{Q}(\zeta^h) \subset \mathbb{Q}(\zeta)$$

and

$$[\mathbb{Q}(\zeta^h) : \mathbb{Q}] = \deg(\Phi_7(X)) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$$

implies that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^h)] = 1$ and so $\mathbb{Q}(\zeta^h) = \mathbb{Q}(\zeta)$. So we have shown that $\sigma \in \operatorname{Gal}(E/K)$ with $\sigma(\zeta) = \zeta^h$, as required. Hence

$$\operatorname{Gal}(E/\mathbb{Q}) \cong \operatorname{im}\rho = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}.$$

In particular, $|\operatorname{Gal}(E/\mathbb{Q})| = 6$ and $\operatorname{Gal}(E/\mathbb{Q}) < S_6$. We now want to find the group structure of $\operatorname{im}\rho$. Notice that for $k, h \in \{1,2,3,4,5,6\}$ we have

$$\pi_k\pi_h(\zeta) = \pi_k(\zeta^h) = \zeta^{kh} = \zeta^l = \pi_l(\zeta)$$

for some $l \in \{1,2,3,4,5,6\}$ such that $kh \equiv l \pmod 7$. Hence

$$\pi_k\pi_h = \pi_l, \text{ where } kh \equiv l \pmod 7$$

and so the bijection

$$\phi : \operatorname{im}\rho \longleftarrow \mathbb{Z}_7^\times, \quad \phi(\pi_h) = \overline{h}$$

is a group isomorphism, since

$$\phi(\pi_k\pi_h) = \phi(\pi_l) = \overline{l} = \overline{kh} = \overline{k}\overline{h} = \phi(\pi_k)\phi(\pi_h)$$

for all $k, h \in \{1,2,3,4,5,6\}$. We know that $\mathbb{Z}_7^\times$ is cyclic and since $\operatorname{im}\rho \cong \mathbb{Z}_7^\times$, we have $\operatorname{im}\rho \cong C_6$. Hence $\operatorname{Gal}(E/\mathbb{Q}) \cong C_6$.

(b) We first find a generator of $\operatorname{Gal}(E/\mathbb{Q})$. For this we need an element of order 6. Notice that π_3 satisfies

$$\zeta^1 \xrightarrow{\pi_3} \zeta^3 \xrightarrow{\pi_3} \zeta^2 \xrightarrow{\pi_3} \zeta^6 \xrightarrow{\pi_3} \zeta^4 \xrightarrow{\pi_3} \zeta^5 \xrightarrow{\pi_3} \zeta^1$$

and so $\operatorname{Gal}(E/\mathbb{Q})$ is generated by $\sigma = \pi_3$. The subgroups of a finite cyclic group correspond to the divisors of the order of the group. Hence for the divisor graph

$$\begin{array}{ccc} & 6 & \\ / & & \backslash \\ 2 & & 3 \\ \backslash & & / \\ & 1 & \end{array}$$

we have the subgroup inclusions graph

$$\begin{array}{ccc} & \{\mathbb{1}_E\} = \langle\sigma^6\rangle & \\ \nearrow & & \nwarrow \\ \langle\sigma^2\rangle & & \langle\sigma^3\rangle \\ \nwarrow & & \nearrow \\ & \operatorname{Gal}(E/\mathbb{Q}) = \langle\sigma^1\rangle & \end{array}$$

corresponding to the intermediate fields inclusion graph

$$\begin{array}{ccccc} & & E & & \\ & \subset & & \supset & \\ E^{\langle \sigma^2 \rangle} & & & & E^{\langle \sigma^3 \rangle}. \\ & \supset & & \subset & \\ & & \mathbb{Q} & & \end{array}$$