10pt **Cf. 14.2.28.** *Let $f \in F[x]$ be an irreducible polynomial of degree n over a field F, let α be a root of f, and let K/F be a normal extension. Show that f splits over K into a product of irreducible polynomials of the same degree $d = [K(\alpha) : K]$. (You may assume that f is separable and K/F is finite and separable.)*

Solution. First, assume that f is separable. Let L be a splitting field of f over K, let E/F be the Galois closure of K/F. Let $f = f_1 \cdots f_m$ be the factorization of f to irreducible components over K. Let α be a root of f_1, let $i \in \{2, \dots, m\}$, and β be a root of f_i. Since α and β are two roots of the same irreducible polynomial f, there exists an automorphism $\varphi \in \mathrm{Gal}(E/F)$ such that $\varphi(\alpha) = \beta$; since K is normal, $\varphi(K) = K$, so φ maps f_1 to a polynomial irreducible over K and having β as a root, that is, $\varphi(f_1) = f_i$. This implies that $\deg f_i = f_1$, that is, the polynomials $f_1, \dots, f_m$ have the same degree $d = n/m = [K(\alpha) : K]$.

If f is not separable, then $f(x) = g(x^{p^k})$ for some separable $g \in F[x]$ (where $p = \mathrm{Char}\, F$), g splits over K into a product of irreducible polynomials of the same degree, and so does f.

Cf. 14.6.20. *Let K be the splittig field of $f(x) = (x^3 - 2)(x^3 - 3) \in \mathbb{Q}[x]$, let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{3}$, $\omega = e^{2\pi i/3}$.*

10pt (a) *Consider K as the composite $\mathbb{Q}(\alpha, \omega)\mathbb{Q}(\beta)$ and represent G as a semidirect product of S_3 and $\mathbb{Z}_3$. (Don't specify the homomorphism that defines the semidirect product, if you don't want to.)*

Solution. The splitting field K of f is $K = \mathbb{Q}(\alpha, \beta, \omega) = \mathbb{Q}(\alpha, \omega)\mathbb{Q}(\beta)$. We have the following (noncomplete!) diagrams of subfields of K and of the corresponding subgroups of G:

$$\begin{tikzcd}[column sep=small]
& K \arrow[dl, equal, "3"'] \arrow[dr, equal, "6"] & \\
\mathbb{Q}(\alpha,\omega) \arrow[dr, equal, "6"'] & & \mathbb{Q}(\beta) \arrow[dl, dash, "3"] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[column sep=small]
& 1 \arrow[dl, equal, "3"'] \arrow[dr, equal, "6"] & \\
H \arrow[dr, equal, "6"'] & & M \arrow[dl, dash, "3"] \\
& G &
\end{tikzcd}$$

(The degrees of the extensions are obtained from the fact that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, and ω, being non-real, has degree 2 over each of $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$, and $\mathbb{Q}(\alpha, \beta)$.) $\mathbb{Q}(\alpha, \omega)$ is the splitting field of $x^3 - 2$, so the extension $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ is normal, H is normal in G, and, as we know, $G/H = \mathrm{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) \cong S_3$. Since $|H| = [K : \mathbb{Q}(\alpha, \omega)] = 3$, $H \cong \mathbb{Z}_3$, and by the theorem about a "free composite of two extensions one of which is normal", G is (isomorphic to) a non-direct semidirect product $\mathbb{Z}_3 \rtimes S_3$. Since there is only one nontrivial automorphism, of order 2, of $\mathbb{Z}_3$, such a semidirect product is unique: if $S_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1,\ \tau\sigma\tau = \sigma^2 \rangle$ and $\mathbb{Z}_3 = \langle \varphi \mid \varphi^3 = 1 \rangle$, then it must be that $\sigma\varphi\sigma^{-1} = \varphi$ and $\tau\varphi\tau^{-1} = \varphi^2$, so

$$G = \langle \varphi, \sigma, \tau : \varphi^3 = \sigma^3 = \tau^2 = 1,\ \tau\sigma\tau = \sigma^2,\ \tau\varphi\tau = \varphi^2 \rangle$$

(which can also be seen as $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$).

Let us, however, describe the elements of G in terms of their action on α, β, ω. Since $|G| = [K : \mathbb{Q}] = 18$, any choice of the conjugates of these elements defines an element of G. Put $\sigma\colon \left(\begin{smallmatrix} \alpha \mapsto \omega\alpha \\ \beta \mapsto \beta \\ \omega \mapsto \omega \end{smallmatrix}\right)$, $\tau\colon \left(\begin{smallmatrix} \alpha \mapsto \alpha \\ \beta \mapsto \beta \\ \omega \mapsto \omega^2 \end{smallmatrix}\right)$, $\varphi\colon \left(\begin{smallmatrix} \alpha \mapsto \alpha \\ \beta \mapsto \omega\beta \\ \omega \mapsto \omega \end{smallmatrix}\right)$. Then $|\sigma| = |\varphi| = 3$, $|\tau| = 2$, $\sigma\varphi = \varphi\sigma$. Also $\tau\sigma\tau\colon \left(\begin{smallmatrix} \alpha \mapsto \omega^2\alpha \\ \beta \mapsto \beta \\ \omega \mapsto \omega \end{smallmatrix}\right) = \sigma^2$ and $\tau\varphi\tau\colon \left(\begin{smallmatrix} \alpha \mapsto \alpha \\ \beta \mapsto \omega^2\beta \\ \omega \mapsto \omega \end{smallmatrix}\right) = \varphi^2$.

10pt (b) *Consider K as the composite $\mathbb{Q}(\alpha, \omega)\mathbb{Q}(\beta, \omega)$ and represent G as a "relative direct product" $S_3 \times_{\mathbb{Z}_2} S_3$.*

Solution. This time we use the following diagrams of subfields of K/subgroups of G:

$$\begin{tikzcd}[column sep=small]
& K \arrow[dl, equal, "3"'] \arrow[dr, equal, "3"] & \\
\mathbb{Q}(\alpha,\omega) \arrow[dr, equal, "3"'] & & \mathbb{Q}(\beta,\omega) \arrow[dl, equal, "3"] \\
& \mathbb{Q}(\omega) \arrow[d, equal, "2"] & \\
& \mathbb{Q} &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[column sep=small]
& 1 \arrow[dl, equal, "3"'] \arrow[dr, equal, "3"] & \\
H_1 \arrow[dr, equal, "3"'] & & H_2 \arrow[dl, equal, "3"] \\
& P \arrow[d, equal, "2"] & \\
& G &
\end{tikzcd}$$

The extensions $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\omega)$ and $\mathbb{Q}(\beta, \omega)/\mathbb{Q}(\omega)$ are normal with both $\mathrm{Gal}\big(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}\big) \cong S_3$ and $\mathrm{Gal}\big(\mathbb{Q}(\beta, \omega)/\mathbb{Q}\big) \cong S_3$. We have the homomorphism $\eta\colon G \longrightarrow \mathrm{Gal}\big(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}\big) \times \mathrm{Gal}\big(\mathbb{Q}(\beta, \omega)/\mathbb{Q}\big)$ defined by

$\eta(\varphi) = \big(\varphi|_{\mathbb{Q}(\alpha,\omega)}, \varphi|_{\mathbb{Q}(\beta,\omega)}\big)$. Since every $\varphi \in G$ is defined by its action on $\mathbb{Q}(\alpha,\omega)$ and $\mathbb{Q}(\beta,\omega)$, η is injective. Since $|G| = 18$ and $|S_3 \times S_3| = 36$, η cannot be surjective; and indeed, if $(\psi_1,\psi_2) = \eta(\varphi)$, then $\psi_1|_{\mathbb{Q}(\omega)} = \varphi|_{\mathbb{Q}(\omega)} = \psi_2|_{\mathbb{Q}(\omega)}$, so the images of ψ_1 and of ψ_2 in the quotient group $G/P = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_2$, where $P = \mathrm{Gal}(K/\mathbb{Q}(\omega))$, coincide. So, $\eta(G)$ is contained in the subgroup $G' = \big\{(\psi_1,\psi_2) : \psi_1 \bmod P = \psi_2 \bmod P\big\}$ of $\mathrm{Gal}\big(\mathbb{Q}(\alpha,\omega)/\mathbb{Q}\big) \times \mathrm{Gal}\big(\mathbb{Q}(\beta,\omega)/\mathbb{Q}\big)$, and since $|G'| = 18 = |G|$, we have $G = G'$.

5pt (c) *Find all the subfields of K that contain $N = \mathbb{Q}(\omega)$.*

Solution. The subfields of K containing N correspond to the subgroups of $P = \mathrm{Gal}(K/N)$. We have $P \cong \mathbb{Z}_3^2$, this is a 2-dimensional $\mathbb{F}_3$-vector space, and its subgroups are its subspaces. In addition to 0 (i.e.1) and itself, P has $(9-1)/2 = 4$ 1-dimensional subspaces (each subspace is defined by a nonzero element of P with only two nonzero elements in each subspace), and so, 4 nontrivial subfields. These clearly are $\mathbb{Q}(\alpha,\omega)$, $\mathbb{Q}(\beta,\omega)$, $\mathbb{Q}(\alpha\beta,\omega)$, and $\mathbb{Q}(\alpha^2\beta,\omega)$ (which is the same as $\mathbb{Q}(\alpha\beta^2,\omega)$).

A1. *Let $\alpha = \sqrt{2}+\sqrt{3}+\sqrt{5}$.*

5pt (a) *Find all the conjugates of α over $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$ and find the minimal polynomial $m_{\alpha,L}$.*

Solution. The conjugates of α over L are only $\sqrt{2}+\sqrt{3}\pm\sqrt{5}$, so

$$m_{\alpha,L} = \big(x-(\sqrt{2}+\sqrt{3}+\sqrt{5})\big)\big(x-(\sqrt{2}+\sqrt{3}-\sqrt{5})\big) = (x-\sqrt{2}-\sqrt{3})^2-5 = x^2+2+3-2\sqrt{2}x-2\sqrt{3}x+2\sqrt{6}-5$$
$$= x^2-2\sqrt{2}x-2\sqrt{3}x+2\sqrt{6}.$$

5pt (b) *Find all the conjugates of α over $N = \mathbb{Q}(\sqrt{2})$ and find the minimal polynomial $m_{\alpha,N}$.*

Solution. The minimal polynomial $m_{\alpha,N}$ splits over L into a product of irreducible polynomials, which are the conjugates over N of $m_{\alpha,L}$ and are obtained by applying to $m_{\alpha,L}$ the automorphisms $\sqrt{3} \mapsto \pm\sqrt{3}$; these are $x^2-2\sqrt{2}x-2\sqrt{3}x+2\sqrt{6}$ and $x^2-2\sqrt{2}x+2\sqrt{3}x-2\sqrt{6}$. So,

$$m_{\alpha,N} = \big(x^2-2\sqrt{2}x-2\sqrt{3}x+2\sqrt{6}\big)\big(x^2-2\sqrt{2}x-2\sqrt{3}x+2\sqrt{6}\big) = \big(x^2-2\sqrt{2}x\big)^2-3\big(2x-2\sqrt{2}\big)^2$$
$$= x^4-4\sqrt{2}x^3+8x^2-12x^2-24+24\sqrt{2}x = x^4-4\sqrt{2}x^3-4x^2+24\sqrt{2}x-24.$$

5pt (c) *Find the minimal polynomial $m_{\alpha,\mathbb{Q}}$.*

Solution. It is the product of the conjugates of $m_{\alpha,N}$:

$$m_{\alpha,\mathbb{Q}} = \big(x^4-4\sqrt{2}x^3-4x^2+24\sqrt{2}x-24\big)\big(x^4+4\sqrt{2}x^3-4x^2-24\sqrt{2}x-24\big) = \big(x^4-4x^2-24\big)^2-2\big(4x^3-24x\big)^2$$
$$= x^8+16x^4+24^2-8x^6-48x^4+8\cdot 24x^2-32x^6-2\cdot 24^2x^2+16\cdot 24x^4 = x^8-40x^6+352x^4-960x^2+576.$$

5pt (d) *Prove that α is a primitive element of $\mathbb{Q}\big(\sqrt{2},\sqrt{3},\sqrt{5}\big)/\mathbb{Q}$.*

Solution. Let $K = \mathbb{Q}\big(\sqrt{2},\sqrt{3},\sqrt{5}\big)$. $\deg_{\mathbb{Q}}\alpha = 8 = [K:\mathbb{Q}]$, so $K = \mathbb{Q}(\alpha)$.

10pt **A2.** *Let K be a cubic extension $\mathbb{Q}\big(\sqrt[3]{D}\big)$ of $\mathbb{Q}$. Obtain the formula for the norm $N_{K/\mathbb{Q}}(\alpha)$ of the element $\alpha = a+b\sqrt[3]{D}+c\sqrt[3]{D^2}$, $a,b,c \in \mathbb{Q}$, of K.*

Solution. There are different ways to find the norm of α: by computing the free term of its minimal polynomial, by finding the product of all its conjugates, ... I'll use "the determinant formula": $N_{K/\mathbb{Q}}(\alpha) = \det T$, where T is the operator of multiplication by α. For $\alpha = a+b\sqrt[3]{D}+c\sqrt[3]{D^2}$ in the basis $\big\{1, \sqrt[3]{D}, \sqrt[3]{D^2}\big\}$ the matrix of T is $\begin{pmatrix} a & cD & bD \\ b & a & cD \\ c & b & a \end{pmatrix}$, and $N_{K/\mathbb{Q}}(\alpha) = \det T = a^3+b^3D+c^3D^2-3abcD$.

A3. *Prove the following:*

5pt (a) *If K/F is a p-extension and L/F is a subextension of K/F, then both K/L and L/F are p-extension.*

Solution. Let K/F be a subextension of a Galois extension E/F with $[E:F] = p^n$. Then L/F is also a subextension of E/F, so is a p-extension. And K/L is a subextension of E/L, where E/L is also a Galois p-extension.

5pt (b) *If L_1/F and L_2/F are p-subextensions of an extension K/F, then their composite L_1L_2/F is a p-extension.*

Solution. If L_1/F and L_2/F are towers of Galois extensions of degree p, then L_1L_2/F is also a tower of Galois extensions whose Galois groups are isomorphic to subgroups of $\mathbb{Z}_p$, so are either trivial or isomorphic to $\mathbb{Z}_p$.

5pt (c) *If K/L and L/F are p-extensions, then K/F is also a p-extension.*

Solution. If K/L and L/F are towers of Galois extensions of degree p, then so is K/F.

5pt **14.7.12.** *Let K be a Galois closure of a finite extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ and let $G = \mathrm{Gal}(K/\mathbb{Q})$. For every prime p dividing $|G|$, prove that there exists a subfield L of K such that $[K : L] = p$ and $K = L(\alpha)$.*

Solution. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By Sylow's and Galois's theorems, there exists a subfield L' of K such that $[K : L'] = p$. K is generated by the conjugates of α; if L' contained all these conjugates, then we would have $L' = K$, so there is a conjugate α' of α such that $\alpha' \notin L'$. Since $[K : L']$ is prime, we have $K = L'(\alpha')$. Let $\varphi \in G$ be such that $\varphi(\alpha') = \alpha$. Put $L = \varphi(L')$. Then $[K : L] = [K : L'] = p$, and $L(\alpha) = \varphi(L'(\alpha')) = K$.