

742 Final - Answer Key

1. Let F be the splitting field over the rationals \mathbb{Q} of the polynomial $x^4 - 3$.

a. Find the Galois group $G = \text{Gal}(F/\mathbb{Q})$.

Let α be the real positive fourth root of 3. Then the roots of $x^4 - 3$ are $\pm\alpha$ and $\pm\alpha i$. Hence $F = \mathbb{Q}[\pm\alpha, \pm\alpha i]$. Since $i = \alpha i/\alpha \in F$, it is clear that $F = \mathbb{Q}[\alpha, i]$.

We find the degree $|F : \mathbb{Q}|$ as follows. Since the polynomial $x^4 - 3$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for the prime 3, we have $|\mathbb{Q}[\alpha] : \mathbb{Q}| = 4$. Next, i satisfies $x^2 + 1$ over \mathbb{Q} and hence over $\mathbb{Q}[\alpha]$. But $i \notin \mathbb{Q}[\alpha]$ since we chose α to be real. Thus $x^2 + 1$ is irreducible over $\mathbb{Q}[\alpha]$ and $|\mathbb{Q}[\alpha, i] : \mathbb{Q}[\alpha]| = 2$. It follows that $|F : \mathbb{Q}| = |\mathbb{Q}[\alpha, i] : \mathbb{Q}[\alpha]| \cdot |\mathbb{Q}[\alpha] : \mathbb{Q}| = 8$ and $|G| = 8$.

There are now three different approaches to finding G . Here is the first. Since $F = \mathbb{Q}[\alpha, i]$, any $\sigma \in G$ is uniquely determined by $\sigma(\alpha)$ and $\sigma(i)$. Now σ permutes the roots of $x^4 - 3$, so there are at most four possibilities for $\sigma(\alpha)$, namely $\pm\alpha$ or $\pm\alpha i$. Similarly, σ permutes the roots of $x^2 + 1$, so there are at most two possibilities for $\sigma(i)$, namely $\pm i$. Thus there are at most $4 \cdot 2 = 8$ possibilities for the action of σ . But $|G| = 8$, so there are 8 such elements and hence all 4·2 possibilities occur. In other words, we can choose any $\pm\alpha, \pm\alpha i$ and any $\pm i$ and find a unique $\sigma \in G$ that sends α to the first choice and i to the second. We can now label the elements of G by their images of α and i , and then work out the multiplication table. We will do this below in the second approach.

Here is the second way to find G . We know that $|F : \mathbb{Q}[\alpha]| = 2$ and that this extension is the splitting field of $x^2 + 1$. So it is a Galois extension of degree 2 and $\text{Gal}(F/\mathbb{Q}[\alpha])$ is transitive on the roots of $x^2 + 1$. Thus there exists $\sigma \in \text{Gal}(F/\mathbb{Q}[\alpha]) \subseteq G$ with $\sigma(i) = -i$ and $\sigma(\alpha) = \alpha$. Similarly, by degree multiplication, $|F : \mathbb{Q}[i]| = 4$ and since $F = \mathbb{Q}[i][\alpha]$, the polynomial $x^4 - 3$ must be irreducible in $\mathbb{Q}[\alpha][x]$ and F is the splitting field of $x^4 - 3$ over $\mathbb{Q}[\alpha]$. Thus, again by transitivity, there exists $\tau \in \text{Gal}(F/\mathbb{Q}[i]) \subseteq G$ with $\tau(\alpha) = \alpha i$ and $\tau(i) = i$. Note that $\tau^2(\alpha) = \tau(\alpha)\tau(i) = -\alpha$ and $\tau^4(\alpha) = \alpha$, $\tau^4(i) = i$, so $\tau^4 = 1$. Also $\sigma \neq 1$, but $\sigma^2 = 1$. Finally, it is easy to check that $\sigma^{-1}\tau\sigma = \sigma\tau\sigma$ fixes i and maps α to $-\alpha i$, so $\sigma^{-1}\tau\sigma = \tau^3 = \tau^{-1}$. Thus σ and τ generate the dihedral group of order 8 and since G contains $\langle \sigma, \tau \rangle$, we conclude that G is the dihedral group of order 8.

Finally, here is a third approach that is easy but only works in some special cases. We know that G permutes the roots of $x^4 - 3$ and acts faithfully as a permutation group. Thus G is isomorphic to a subgroup of Sym_4 , a group of order $4 \cdot 3 = 12$. But $|G| = 8$, so G is isomorphic to a Sylow 2-subgroup of Sym_4 and this is known to be the dihedral group of order 8 generated by $\tau = (1\ 2\ 3\ 4)$ and $\sigma = (1\ 3)$.

b. If $\alpha \in F$ is a fourth root of 3, show that all G -conjugates of $\beta = \alpha + i$ are distinct. Explain why $F = \mathbb{Q}[\beta]$.

As we have seen, $\alpha \notin \mathbb{Q}[i]$. Thus 1 and α are linearly independent over $\mathbb{Q}[i]$. Since $\sigma(\beta) = \sigma(\alpha) + \sigma(i) = \{\pm 1, \pm i\}\alpha + \{\pm 1\}i$, the linear independence implies that these are all distinct. In particular, if $\sigma \neq 1$, then $\sigma(\beta) \neq \beta$. Thus the subgroup H of G fixing $\mathbb{Q}[\beta]$ is the identity group and the fundamental theorem implies that $\mathbb{Q}[\beta] = F^H = F^1 = F$.

c. Find all intermediate fields $F \supseteq E \supseteq \mathbb{Q}$ with $|E : \mathbb{Q}| = 4$ and E/\mathbb{Q} Galois.

Let $G = \langle \tau, \sigma \mid \tau^4 = 1, \sigma^2 = 1, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle$ be the dihedral group of order 8 and set $Z = \langle \tau^2 \rangle$. Then $Z = G'$ is central in G and G/Z is the fours group. In particular, G has three subgroups of order 4 containing Z , namely $G_1 = \langle \tau \rangle$, $G_2 = \langle \tau^2, \sigma \rangle$, and $G_3 = \langle \tau^2, \sigma\tau \rangle$. Since none of these is central in G , Z is the center of G .

Now if E is as above, then $E = F^H$ where H is a normal subgroup of G of order 2. But any normal subgroup of order 2 is clearly central, so $H = Z$ is the unique possibility and $E = F^H = F^Z = F^{\langle \tau^2 \rangle} = \mathbb{Q}[i, \alpha^2]$.

d. Find all intermediate fields $F \supseteq K \supseteq \mathbb{Q}$ with $|K : \mathbb{Q}| = 2$.

Here $K = F^H$ where H is a subgroup of G of index 2. Thus H is normal in G and G/H is abelian, so $H \supseteq G' = Z$. This implies that $H = G_1, G_2$ or G_3 as given above, and there are three possibilities for K , namely $F^{G_1} = \mathbb{Q}[i]$, $F^{G_2} = \mathbb{Q}[\alpha^2]$ and $F^{G_3} = \mathbb{Q}[\alpha^2 i]$.

2. Let $F \supseteq K$ be fields, and let E_1 and E_2 be intermediate fields. Assume that E_1 and E_2 are Galois over K , and that F is generated by E_1 and E_2 .

a. Prove that F/K is Galois.

We know that $E_1 = K[f_1]$ and $E_2 = K[f_2]$, where f_1 and f_2 are monic separable polynomials in $K[x]$. Hence, since F is generated by E_1 and E_2 , it is clear that $F = K[f_1 f_2]$. However, $f_1 f_2$ may have multiple roots.

To deal with this problem, factor f_1 and f_2 into monic irreducible factors in $K[x]$ and let g be the product of the distinct irreducible factors that occur. Then $g \in K[x]$ and clearly $F = K[f_1 f_2] = K[g]$. Recall that distinct irreducible polynomials cannot have a root in common. So to check that g is separable, we need only show that each of its irreducible factors h has distinct roots. But if $h \mid g$, then $h \mid f_1$ or $h \mid f_2$ and hence h has distinct roots. Thus g is separable and $F = K[g]$ is Galois over K .

b. Prove that $\text{Gal}(F/K)$ is isomorphic to a subgroup of $\text{Gal}(E_1/K) \times \text{Gal}(E_2/K)$ that projects fully onto each factor.

Since E_1/K and E_2/K are Galois, the fundamental theorem of Galois theory implies that $G = \text{Gal}(F/K)$ acts on E_1 and E_2 . Thus we have restriction homomorphisms from G to $\text{Gal}(E_1/K)$ and $\text{Gal}(E_2/K)$. Indeed, the fundamental theorem asserts that each of these maps is onto. Combining them, we have a homomorphism $G \rightarrow \text{Gal}(E_1/K) \times \text{Gal}(E_2/K)$. Observe that any $\sigma \in G$ in the kernel of this map fixes both E_1 and E_2 , so it fixes F since they generate that field. Hence $\sigma = 1$ and this homomorphism is one-to-one. Finally, since each map $G \rightarrow \text{Gal}(E_i/K)$ is onto, the image of G in $\text{Gal}(E_1/K) \times \text{Gal}(E_2/K)$ projects fully onto each factor.

3. Let $d \in \mathbb{Z}$ be a square free integer with $d \equiv 1 \pmod{4}$ and $d \neq 1$.

a. Explain why $\mathbb{Z}[\sqrt{d}]$ is not integrally closed.

Let $\alpha = (1 + \sqrt{d})/2$ and $\beta = (1 - \sqrt{d})/2$. Then $\alpha + \beta = 1$ and $\alpha\beta = (1 - d)/4 \in \mathbb{Z}$, so α and β are roots of the monic integer polynomial $(x - \alpha)(x - \beta) = x^2 - x + (1 - d)/4$. Thus α and β are integral over \mathbb{Z} and hence over $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Since $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$, but are not in $\mathbb{Z}[\sqrt{d}]$, the latter ring is not integrally closed.

b. Find a nonzero ideal in $\mathbb{Z}[\sqrt{d}]$ that is not invertible.

It is tedious to show that a particular ideal is not invertible, so we use the proof that invertible ideals implies that the ring is integrally closed. Write $R = \mathbb{Z}[\sqrt{d}]$ and set $X = R1 + R\alpha$, with α as above. Then X is properly larger than R and $X = R[\alpha]$ is a ring, so $X^2 = X$. If $A = 2R$, then $AX = B \subseteq R$. So B is an ideal of R . Indeed, $B = (2)(1, \alpha) = (2, 2\alpha) = (2, 1 + \sqrt{d})$.

If B is invertible, then $B^2 = A^2X^2 = A^2X = AB$ implies, multiplying by B^{-1} , that $A = B$. Then $B = AX = BX$ yields $X = B^{-1}B = R$, a contradiction since $\alpha \notin R$. Thus $B = (2, 1 + \sqrt{d})$ is not invertible in R . Note that, to check directly that $BB^{-1} \neq R$, it is not sufficient to study an equation like $bc = 1$, for some $b \in B$ and $c \in B^{-1}$, since BB^{-1} is a sum of products.

4. Let R be a commutative domain (not a field) with the property that every nonzero ideal is a finite product of maximal ideals.

a. Prove that every nonzero principal ideal is invertible and then that every maximal ideal is invertible.

To prove that an ideal A is invertible, we merely have to show that there exists B with $AB = R$. It then follows that $B = A^{-1}$. If $A = aR$ is principal with $a \neq 0$, take $B = (1/a)R$, so $AB = R$.

Now let M be a maximal ideal of R . Then $M \neq 0$ since R is not a field. Choose $0 \neq a \in M$ and set $A = aR$. By assumption, $A = M_1M_2 \cdots M_n$ is a product of maximal ideals. We have $M \supseteq A = M_1M_2 \cdots M_n$, and M is prime since it is maximal. Thus $M \supseteq M_i$ for some subscript i , and hence $M = M_i$ since M_i is maximal. We can clearly assume that $i = 1$, so $A = MM_2 \cdots M_n$, and $R = M(M_2 \cdots M_n)A^{-1}$. It follows from our previous comments that M is invertible.

b. Deduce that R is a Dedekind domain.

If A is a nonzero ideal of R , then by assumption, $A = M_1M_2 \cdots M_n$ is a finite product of maximal ideals. But each M_i is invertible by the above, so $A \cdot M_1^{-1}M_2^{-1} \cdots M_n^{-1} = R$ and hence A is invertible. Since all nonzero ideals of R are invertible, we know that R is a Dedekind domain.