Solution 15

Definition of Galois group

1. Let E/k be a field extension. Show that every $\sigma \in \mathrm{Gal}(E/k)$ is an invertible k-linear map of the $k-$vector space E.

   Solution: By definition, $\sigma \in \mathrm{Gal}(E/k)$ is a field automorphism of E which is the identity on k. In particular, it is a bijective map. In order to conclude, we show k-linearity. For every $\lambda \in k$ and $x, y \in E$,

   $$\sigma(x + \lambda y) = \sigma(x) + \sigma(\lambda y) = \sigma(x) + \sigma(\lambda)\sigma(y) = \sigma(x) + \lambda\sigma(y),$$

   which means that σ is a k-linear map. Notice that in the first two equalities we used the fact that σ respects sum and multiplication (it is a ring homomorphism), while in the last one we used the fact that $\sigma|_k = \mathrm{id}_k$.

2. Show that $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$, where σ is complex conjugation.

   Solution: The inclusion $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \supset \{\mathrm{id}, \sigma\}$ is clear, since we already know that the identity and the complex conjugation are automorphisms of $\mathbb{C}$ fixing the real numbers.

   Conversely, assume that $\varphi \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is a field automorphism. Since φ is $\mathbb{R}$-linear by Exercise 1), it is uniquely determined by the images of 1 and i. Moreover, since $\varphi|_{\mathbb{R}} = \mathrm{id}|_{\mathbb{R}}$, we know that

   $$\varphi(1) = 1 \text{ and } \varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1 \implies \varphi(i) \in \{\pm i\}.$$

   This implies that there are at most 2 elements in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, so that we can conclude that $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$.

3. Determine all irreducible polynomials of degree $1, 2, 3, 4, 5$ in $\mathbb{F}_2[X]$.

   Solution: Recall that, over an integral domain R, for two polynomials $f, g \in R[X]$ we know that $\deg(fg) = \deg(f)\deg(g)$. Moreover, $R[X]^\times = R^\times$, so that if R is also a field, then a polynomial $f \in R[X]$ is irreducible if and only if it admits no decomposition into two non-constant polynomials (e.g., this fails on $R = \mathbb{Z}$, where the polynomial $2X + 2 = 2(X + 1)$ is reducible because 2 is not a unit, although it is constant).

   - Because of the facts recalled above, all polynomials of degree 1 in $\mathbb{F}_2[X]$ are irreducible. Those are

     $$X,\ X + 1.$$

- For polynomials of degree 2 and 3, being reducible is equivalent to have a linear factor, because a decomposition of such a polynomial into the product of two non-constant polynomials implies that one of the two has degree 1. Moreover, having a linear factor is equivalent to having a root in $\mathbb{F}_2$. We see that $f \in \mathbb{F}_2[X]$ satisfies $f(0) = 0$ if and only if its constant term is 0 and it satisfies $f(1) = 0$ if and only if the sum of the coefficients is 0, i.e., there is an even number of non-zero coefficients. Hence, we look for polynomials of degree 2 and 3 satisfying neither of those two properties and conclude that the irreducible polynomials in $\mathbb{F}_2[X]$ of degree 2 and 3 are

$$X^2 + X + 1,\ X^3 + X^2 + 1,\ X^3 + X + 1.$$

- A polynomial $f \in \mathbb{F}_2[X]$ of degree 4 is irreducible if and only if it has no roots (i.e., no factor of degree 1) and it is not the product of two irreducible polynomials of degree 2 (if one of the two degree-2 polynomials is reducible, we fall again in the case where f has a linear factor). This means that we look for all polynomials $f \in \mathbb{F}_2[X]$ of degree 4 with constant term 1 and odd number of non-zero coefficients and then remove from those the polynomial $(X^2+X+1)(X^2+X+1) = X^4+X^2+1$. This way we obtain the irreducible degree-4 polynomials

$$X^4 + X^3 + 1,\ X^4 + X + 1,\ X^4 + X^3 + X^2 + X + 1.$$

- A polynomial $f \in \mathbb{F}_2[X]$ of degree 5 is irreducible if and only if it has no roots (i.e., no factor of degree 1) and it is not the product of an irreducible polynomials of degree 2 by an irreducible polynomial of degree 3 (if one of those two polynomials is reducible, we fall again in the case where f has a linear factor). Hence we look for all polynomials $f \in \mathbb{F}_2[X]$ of degree 5 with constant term 1 and odd number of non-zero coefficients and then remove from those the polynomials $(X^2 + X + 1)(X^3 + X^2 + 1) = X^5 + X + 1$ and $(X^2+X+1)(X^3+X+1) = X^5+X^4+1$. This way we obtain the irreducible degree-5 polynomials

$$X^5 + X^4 + X^3 + X^2 + 1,\ X^5 + X^4 + X^3 + X + 1,\ X^5 + X^4 + X^2 + X + 1,$$
$$X^5 + X^3 + X^2 + X + 1,\ X^5 + X^3 + 1,\ X^5 + X^2 + 1.$$

4. Show that $X^4 + 1 \in \mathbb{Q}[X]$ is irreducible. Show that $X^4 + 1$ is reducible in $\mathbb{F}_p[X]$ for every prime p.

   Solution: The standard approach to prove that $X^4 + 1$ is irreducible in $\mathbb{Q}$ is to first notice that it has no rational roots (in this case, it is clear that it even has no real roots) and then to suppose it is the product of two degree-2 polynomials with rational coefficients, i.e, that there exist $a, b, c, d \in \mathbb{Q}$ such that

$$X^4 + 1 = (X^2 + aX + b)(X^2 + bX + d) \tag{1}$$

and get a contraddiction by comparing coefficients.

In order to exclude this second possibility, we notice that a decomposition (1) would be a decomposition in $\mathbb{C}[X]$ as well. Denoting by $z_1, \dots, z_4$ the four roots of X^4+1 in $\mathbb{C}$, the decomposition

$$X^4+1 = (X-z_1)(X-z_2)(X-z_3)(X-z_4)$$

holds as well, so that, since $\mathbb{C}[X]$ is a UFD, we must have $(X-z_i)(X-z_j) = X^2+aX+b$ for some distinct i and j. Hence

$$X^2+aX+b = X^2-(z_i+z_j)X+z_iz_j \implies z_i+z_j, z_iz_j \in \mathbb{Q} \tag{2}$$

It is easy to compute that

$$\{z_1,z_2,z_3,z_4\} = \left\{ \pm\frac{\sqrt{2}}{2}(1\pm i) \right\}.$$

We see that $z_i+z_j = 0$ if z_i and z_j are opposites, while otherwise $z_i+z_j \in \{\pm\sqrt{2}, \pm\sqrt{2}i\}$. Hence $z_i+z_j \in \mathbb{Q}$ implies that $z_i = -z_j$. But then

$$z_iz_j = -\frac{1}{2}(1\pm i)^2 = -\frac{1}{2}(1\pm i)^2 = -(\pm i) \notin \mathbb{Q}.$$

This contradicts (2), so that X^4+1 is irreducible in $\mathbb{Q}[X]$.

Now we move to $\mathbb{F}_p[X]$. If $p=2$, the polynomial X^4+1 factors as $X^4+1 = (X+1)^4$. So from now on we suppose that $p \geqslant 3$.

Suppose that -1 is a square in $\mathbb{F}_p$, that is, there exists $\xi \in \mathbb{F}_p$ such that $\xi^2 = -1$. Then

$$X^4+1 = (X^2-\xi)(X^2+\xi)$$

so that the given polynomial is reducible and we are left to consider the case in which $p \geqslant 3$ and -1 is not a square.

We denote by $\mathbb{F}_p^{\times 2}$ the subgroup of $\mathbb{F}_p^\times$ consisting of squares. It is the image of the group homomorphism $\theta : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ sending $x \mapsto x^2$. Since $\ker(\theta) = \{\pm 1\}$, by the First Isomorphism Theorem we see that $[\mathbb{F}_p^\times : \mathbb{F}_p^{\times 2}] = 2$. By assumption, $-1 \notin \mathbb{F}_p^{\times 2}$ so that $\mathbb{F}_p^\times = \mathbb{F}_p^{\times 2} \sqcup (-1)\mathbb{F}_p^{\times 2}$. We look for a decomposition of the form

$$X^4+1 = (X^2+aX+b)(X^2-aX+b),\ a,b \in \mathbb{F}_p.$$

This works if and only if $2b-a^2 = 0$ and $b^2 = 1$. Clearly this implies that $a, b \in \mathbb{F}^\times$. More precisely, we obtain $b = \pm 1$ and we need to find $a \in \mathbb{F}_p^\times$ such that $a^2 = 2b$. This works because of the partition $\mathbb{F}_p^\times = \mathbb{F}_p^{\times 2} \sqcup (-1)\mathbb{F}_p^{\times 2}$, which tells us that either 2 or -2 is a square, so that we can choose a to be the square root of one of the two and $b \in \{\pm 1\}$ accordingly.