Solutions Review exercise sheet

1. 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 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

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

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 $z_1, \ldots, z_4$ 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.

2. For the polynomial $X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$ determine the Galois group of its splitting field over $\mathbb{Q}$.

Solution: The polynomial $f = X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$ has no root in $\mathbb{Z}$, since a root would divide the constant term 1, and $f(\pm 1) \neq 0$ because it is an odd integer. Hence it also has no root in $\mathbb{Q}$.

If $x \in \mathbb{C}$ is a root of f, then so is x^{-1}. For $x \neq \pm 1$, we know that $x^{-1} \neq x$, but $f(\pm 1) \neq 0$. Hence the roots of f in $\mathbb{C}$ are given by $a_1, a_1^{-1}, a_2, a_2^{-1}$ for some eventually equal $a_1, a_2 \in \mathbb{C}$. Since $(X - a_j)(X - a_j^{-1}) = X^2 - (a_j + a_j^{-1})X + 1$ for $j = 1, 2$, we can define $\alpha_j := -(a_j + a_j^{-1})$ which lets us write down the decomposition

$$X^4 + 2X^3 + X^2 + 2X + 1 = f = (X^2 + \alpha_1 X + 1)(X^2 + \alpha_2 X + 1).$$

Comparing the coefficients in this equality we obtain the system of equations

$$\begin{cases} \alpha_1 + \alpha_2 = 2 \\ \alpha_1\alpha_2 + 2 = 1 \end{cases}$$

Hence α_1 and α_2 are the two roots of the equation (in α) $\alpha^2 - 2\alpha - 1 = 0$, that is,

$$\alpha_{1,2} = 1 \pm \sqrt{1+1} = 1 \pm \sqrt{2}.$$

This gives us the only decomposition of f into monic polynomials. The roots of f are the roots of the two equations $x^2 + (1 \pm \sqrt{2})x + 1 = 0$, that is the roots of f are given by

$$\left\{ \frac{1}{2}(-1 - \sqrt{2} \pm \sqrt{-1 + 2\sqrt{2}}), \frac{1}{2}(-1 + \sqrt{2} \pm i\sqrt{1 + 2\sqrt{2}}) \right\}.$$

Hence f can not be written as a product of polynomials of degree 2 and is irreducible over $\mathbb{Q}$.

Denote by

$$a_1 = \frac{1}{2}(-1 - \sqrt{2} + \sqrt{-1 + 2\sqrt{2}})$$
$$a_2 = \frac{1}{2}(-1 + \sqrt{2} + i\sqrt{1 + 2\sqrt{2}}).$$

Hence $[\mathbb{Q}(a_1) : \mathbb{Q}] = 4$ and we have that $[\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)] = 2$, since a_2 is a root of $x^2 + (1 - \sqrt{2})x + 1$ and $1 - \sqrt{2} \in \mathbb{Q}(a_1)$. Thus $|\operatorname{Gal}(E : \mathbb{Q})| = 8$, where E is the splitting field of f over $\mathbb{Q}$.

This means that $\mathrm{Gal}(E/\mathbb{Q})$, seen as a subgroup of S_4, is precisely the subgroup W_2 of permutations respecting the partition $\{1, 2, 3, 4\} = \{1, 3\} \cup \{2, 4\}$. This is given by

$$W_2 = \{\mathrm{id}, (1\,3)(2\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1\,4\,3\,2), (1\,3), (2\,4)\},$$

which by numbering the vertices of a square counterclockwise from 1 to 4 can be seen to be isomorphic to D_4, the dihedral group on 4 elements.

3. Let $p > 2$ be a prime number and $\zeta := e^{\frac{2\pi i}{p}}$. Let $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

(a) Show that there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ of order 2. What is its generator? [*Hint:* It is an element of order 2]

(b) Prove that $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq E^H$ and that $[E : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$.

(c) Deduce that $E^H = \mathbb{Q}(\zeta + \zeta^{-1})$.

Solution: An isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ is given by $k + p\mathbb{Z} \mapsto (\zeta \mapsto \zeta^k)$ for each $k \in \mathbb{Z}$. Recall that an automorphism of $\mathbb{Q}(\zeta)$ (fixing $\mathbb{Q}$) is indeed uniquely determined by the image of ζ, which in turn needs to be another root of $\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1$.

(a) By Algebra I, we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$ because $\mathbb{Z}/p\mathbb{Z}$ is a finite field. And $p - 1$ is divisible by 2 since p is odd. Hence $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ has a unique subgroup of order 2. It is generated by the $\frac{p-1}{2}$-th power of a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$. Only one element $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ can have order 2, because two distinct such elements generate distinct subgroups of order 2.
We also know that complex conjugation $\sigma : x \mapsto \overline{x}$ belongs to $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ which clearly has order 2, so that $H = \langle\sigma\rangle$.

(b) As $|\zeta| = 1$, we see that $\zeta^{-1} = \overline{\zeta}$, so that σ actually corresponds to the class of $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$.
We have

$$\sigma(\zeta + \zeta^{-1}) = \sigma(\zeta) + \sigma(\zeta^{-1}) = \zeta^{-1} + \zeta,$$

so that $\zeta + \zeta^{-1} \in E^H$. As E^H is a subfield of E, we can conclude that $\mathbb{Q}(\zeta + \zeta^{-1}) \subset E$. Notice that ζ is a root of $(X - \zeta)(X - \zeta^{-1}) = X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$, so that $[E : \mathbb{Q}(\zeta + \zeta^{-1}] \leqslant 2$.

(c) By the Galois correspondence $[E : E^H] = |H| = 2$. Hence we know that

$$2 \cdot [E^H : \mathbb{Q}(\zeta + \zeta^{-1})] = [E : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$$

so that $[E^H : \mathbb{Q}(\zeta + \zeta^{-1})] = 1$, meaning that $E^H = \mathbb{Q}(\zeta + \zeta^{-1})$.

4. Let $E : k$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(E : k)$ of degree $n = [E : k]$. Define the *trace* $T : E \longrightarrow E$ by

$$T(x) = \sum_{\sigma \in G} \sigma(x).$$

(a) Prove that $\text{im}(T) \subseteq k$ and that T is k-linear.

(b) Show that T is not identically zero and deduce that $\dim(\ker(T)) = n - 1$.

(c) Now suppose that $\mathrm{Gal}(E : k)$ is cyclic and generated by an automorphism σ. Consider the linear map $\tau = \sigma - \mathrm{id}_E$. Prove that

$$\ker(T) = \text{im}(\tau) = \{\sigma(u) - u : u \in E\}.$$

Solution:

(a) Let $\tau \in G$. For each $x \in E$,

$$\tau(T(x)) = \tau\left(\sum_{\sigma \in G} \sigma(x)\right) = \sum_{\sigma \in G} \tau\sigma(x) = T(x),$$

because $\sigma \mapsto \tau\sigma$ is a bijection $G \longrightarrow G$. By arbitrarity of τ and $x \in E$, the image of T is in E^G, which coincides with k because $E : k$ is Galois.
In order to prove that T is k-linear, let $x, y \in E$ and $a \in k$. Then

$$T(x + ay) = \sum_{\sigma \in G} \sigma(x + ay) = \sum_{\sigma \in G} (\sigma(x) + a\sigma(y)) = T(x) + aT(y).$$

(b) The map $T \in \text{Hom}(E^\times, E)$ is a non-trivial linear combination of the finitely elements $\sigma \in \mathrm{Gal}(E : k) = \text{Aut}_k(E^\times)$. Hence $T \neq 0$. Then the image of T is a non-zero k-linear subspace of k, since we have seen in the Single Choice 10 Exercise 2b) that $\text{im}(T) = k$, so that $\dim(\text{im}(T)) = 1$. Then by the First Isomorphism theorem we conclude

$$\dim(\ker(T)) = n - \dim(\text{im}(T)) = n - 1.$$

(c) We notice that $\ker(\tau) = \{u \in E : \sigma(u) = u\} = E^G = k$, because σ generates G so that the elements of E fixed by σ are fixed by the whole G. Again from the First Isomorphism theorem, we obtain

$$\dim(\text{im}(\tau)) = n - \dim(\ker(\tau)) = n - 1.$$

As $\ker(T)$ and $\text{im}(\tau)$ have the same dimension, it suffices to show that one is contained in the other. We show that $\text{im}(\tau) \subset \ker(T)$: for all $x \in E$,

$$T(\sigma(x) - x) = \sum_{\sigma' \in G} \sigma'(\sigma(x) - x) = \sum_{\sigma' \in G} \sigma'\sigma(x) - \sum_{\sigma' \in G} \sigma'(x) = T(x) - T(x) = 0.$$

5. Let p be an odd prime number. Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E : \mathbb{Q}) \cong \mathbb{F}_p^\times$. For $a \in \mathbb{F}_p^\times$, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } a \text{ is a not square in } \mathbb{F}_p^\times. \end{cases}$$

Define the complex number

$$\tau = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a.$$

(a) Show that the map $\mathbb{F}_p^\times \to \{\pm 1\}$ sending $a \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism.

(b) Prove that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p,$$

and that this determines $\left(\frac{a}{p}\right) \in \{\pm 1\}$ uniquely.

(c) Show that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.

(d) For $b \in \mathbb{F}_p^\times$, let $\sigma_b \in \mathrm{Gal}(E : \mathbb{Q})$ be the automorphism $\sigma_b(\zeta) = \zeta^b$. Prove the equality $\sigma_b(\tau) = \left(\frac{b}{p}\right) \cdot \tau$.

(e) Prove that $\mathbb{Q}(\tau) : \mathbb{Q}$ is the unique quadratic intermediate extension of $E : \mathbb{Q}$.

We now want to determine the extension $\mathbb{Q}(\tau)$ by computing τ^2 explicitly.

(f) Let $c \in \mathbb{F}_p^\times$. Show that

$$\sum_{a \in \mathbb{F}_p^\times} \zeta^{a(1+c)} = \begin{cases} -1 & \text{if } c \neq p-1 \\ p-1 & \text{if } c = p-1 \end{cases}$$

(g) Write

$$\tau^2 = \sum_{a \in \mathbb{F}_p^\times} \sum_{b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Substituting $b = ac$ with $c \in \mathbb{F}_p^\times$, deduce that

$$\tau^2 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1).$$

(h) Conclude: if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$; if $p \equiv 3 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$.

Solution:

(a) The group $\mathbb{F}_p^\times$ is cyclic of even order $p-1$. Since it is abelian, the map $s : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ sending $x \mapsto x^2$ is a group homomorphism. The set of squares in $\mathbb{F}_p^\times$ is given by

$$S = \{s(x),\, x \in \mathbb{F}_p^\times\} = \mathrm{im}(s).$$

By the First Isomorphism theorem, s induces an isomorphism $\mathbb{F}_p^\times / \ker(s) \xrightarrow{\sim} S$. Moreover $\ker(s) = \{x \in \mathbb{F}_p^\times : x^2 = 1\} = \{\pm 1\}$ because it contains the roots of the degree-2 polynomial $X^2 - 1 \in \mathbb{F}_p[X]$. Hence S is a subgroup of order 2 of $\mathbb{F}_p^\times$, implying that for $a, b \in \mathbb{F}_p^\times$ the element $ab \in \mathbb{F}_p^\times$ is a square if and only if a and b are both square or both are not squares. In particular, the given map is a group homomorphism.

(b) The group $\mathbb{F}_p^\times$ is the set of roots of $X^{p-1} - 1 \in \mathbb{F}_p[X]$. Since $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$, we know that precisely $\frac{p-1}{2}$ elements in $a \in \mathbb{F}_p^\times$ satisfy $a^{\frac{p-1}{2}} = 1$, the others satisfying $a^{\frac{p-1}{2}} = -1$. If $a = b^2$ for $b \in \mathbb{F}_p^\times$, then $a^{\frac{p-1}{2}} = b^{2 \cdot \frac{p-1}{2}} = 1$. Since by part (a) there are precisely $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$, we conclude that $a^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p$ when a is not a square. Hence $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ for each $a \in \mathbb{F}_p^\times$.

(c) By part (b),

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

which is 1 if and only if $p-1$ is divisible by 4, that is, if and only if $p \equiv 1 \pmod 4$.

(d) The power ζ^a for $a \in \mathbb{F}_p$ is well defined, because $\zeta^{pm} = 1$ for each $m \in \mathbb{Z}$. Clearly, $\tau \in E$ by definition. For each $b \in \mathbb{F}_p^\times$, we compute

$$\begin{aligned}\sigma_b(\tau) = \sigma_b\left(\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\zeta^a\right) &= \sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\sigma_b(\zeta)^a = \sum_{a\in\mathbb{F}_p^\times}\left(\frac{b}{p}\right)\left(\frac{b}{p}\right)\left(\frac{a}{p}\right)\zeta^{ba}\\ &= \left(\frac{b}{p}\right)\sum_{a\in\mathbb{F}_p^\times}\left(\frac{ba}{p}\right)\zeta^{ba} = \left(\frac{b}{p}\right)\tau,\end{aligned}$$

in the last step having used the fact that $\{ba : a \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$ for each $b \in \mathbb{F}_p^\times$, which holds because $\mathbb{F}_p^\times$ is a group.

(e) By part (d), we see that $\sigma_b(\tau^2) = \left(\frac{b}{p}\right)^2\tau^2 = \tau^2$ for each $b \in \mathbb{F}_p$, so that $\tau^2 \in E^{\mathrm{Gal}(E:\mathbb{Q})} = \mathbb{Q}$. Moreover, $\sigma_b(\tau) \neq \tau$ when b is not a square in $\mathbb{F}_p^\times$ (which is the case for half of the elements of $\mathbb{F}_p^\times$), so that $\tau \notin \mathbb{Q}$. Hence $\mathbb{Q}(\tau) : \mathbb{Q}$ is a quadratic extension.

On the other hand, the Galois group $\mathrm{Gal}(E : \mathbb{Q}) \cong \mathbb{F}_p^\times$ is cyclic of even order $p-1$, so it contains precisely one subgroup of index 2 (that is, of order $\frac{p-1}{2}$). Hence, there is precisely one quadratic extension $L : \mathbb{Q}$ contained in E (that is, such that $[E : L] = \frac{p-1}{2}$), which is then given by $\mathbb{Q}(\tau)$.

(f) For $c = p-1$, we get

$$\sum_{a\in\mathbb{F}_p^\times}\zeta^{a(1+c)} = \sum_{a\in\mathbb{F}_p^\times}\zeta^{ap} = \sum_{a\in\mathbb{F}_p^\times}(\zeta^p)^a = \sum_{a\in\mathbb{F}_p^\times}1 = p-1.$$

Else, $1+c \in \mathbb{F}_p^\times$, so that $\{a(1+c) : a \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$ and

$$\sum_{a\in\mathbb{F}_p^\times}\zeta^{a(1+c)} = \sum_{a\in\mathbb{F}_p^\times}\zeta^a = -1 + \sum_{a\in\mathbb{F}_p}\zeta^a = -1,$$

because ζ is a root of $\sum_{a=0}^{p-1}X^a = \frac{X^p-1}{X-1} \in \mathbb{Z}[X]$.

(g) Since $\{ac : c \in \mathbb{F}_p^\times\} = \mathbb{F}_p^\times$, we can perform the suggested substitution, as follows:

$$\begin{aligned}\tau^2 &= \sum_{a\in\mathbb{F}_p^\times}\sum_{b\in\mathbb{F}_p^\times}\left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times}\left(\frac{a(ac)}{p}\right)\zeta^{a+ac} = \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times}\left(\frac{a^2c}{p}\right)\zeta^{a(1+c)}\\ &= \sum_{a\in\mathbb{F}_p^\times}\sum_{c\in\mathbb{F}_p^\times}\left(\frac{c}{p}\right)\zeta^{a(1+c)} = \sum_{c\in\mathbb{F}_p^\times}\left(\frac{c}{p}\right)\sum_{a\in\mathbb{F}_p^\times}\zeta^{a(1+c)} \overset{\text{(f)}}{=} \left(\frac{-1}{p}\right)(p-1) - \sum_{c=1}^{p-2}\left(\frac{c}{p}\right)\end{aligned}$$

(h) The above sum reads

$$\tau^2 = \left(\frac{-1}{p}\right)p - \left(\frac{-1}{p}\right) - \sum_{c=1}^{p-2}\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{c\in\mathbb{F}_p^\times}\left(\frac{c}{p}\right) = \left(\frac{-1}{p}\right)p,$$

because $\left(\frac{c}{p}\right)$ attains the values 1 and -1 an equal number of times for $c \in \mathbb{F}_p^\times$.
If $p \equiv 1 \pmod 4$, then

$$\tau^2 = p,$$

so that $\tau = \pm\sqrt{p}$ and $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$ is a quadratic real extension of $\mathbb{Q}$.
Else, $p \equiv 3 \pmod 4$,

$$\tau^2 = -p,$$

so that $\tau = \pm i\sqrt{p}$ and $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$ is a quadratic imaginary extension of $\mathbb{Q}$.

6. Let $L : K$ be a finite Galois extension with Galois group G. Let G' denote the commutator subgroup $[G,G]$ generated by all commutators $xyx^{-1}y^{-1}$ in G. Show that $L^{G'} : K$ is a Galois extension with $\mathrm{Gal}(L^{G'} : K)$ abelian. Show that any Galois extension $E : K$ with $E \subset L$ and $\mathrm{Gal}(E : K)$ abelian is contained in $L^{G'}$.

Solution: We know that G' is a normal subgroup of G because

$$z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}],$$

so by the Galois correspondence, the extension $L^{G'} : K$ is indeed a Galois extension. Its Galois group is G/G', which is abelian.

If $L : E : K$ is such that $E : K$ is Galois with abelian Galois group, then the subgroup $H = \mathrm{Gal}(L : E)$ is normal with G/H abelian. It follows that $H \supset G'$ (because any commutator maps to 1 in G/H), and therefore by the Galois correspondance that $E \subset L^{G'}$.

7. For all ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ and all elements x, y of a ring R show the formulas

(a) $(x)(y) = (xy)$

(b) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$

(c) $(x) \cdot ((y) \cdot \mathfrak{a}) = (xy) \cdot \mathfrak{a}$

Solution:

(a) Let $r \in (x)(y)$. Then $r = \sum_{i=1}^n x_i y_i$ with $x_i \in (x)$ and $y_i \in (y)$. Write $x_i = a_i x$ and $y_i = b_i y$ for $a_i, b_i \in R$. Then we have

$$r = \sum_{i=1}^n (a_i x)\cdot(b_i y) = \sum_{i=1}^n (a_i b_i)\cdot xy = \left(\sum_{i=1}^n a_i b_i\right)\cdot xy \in (xy).$$

This proves the inclusion $\subset$. For the reverse inclusion we write any $r \in (xy)$ in the form $r = axy = ax \cdot y$ for some $a \in R$. This directly shows that $r \in (x)(y)$, proving the inclusion $\supset$.

(b) Let $x \in \mathfrak{a}(\mathfrak{b}\mathfrak{c})$. Then $x = \sum_{i=1}^{n} a_i d_i$ where $a_i \in \mathfrak{a}$ and $d_i \in \mathfrak{b}\mathfrak{c}$. Similarly each $d_i = \sum_{j=1}^{m_i} b_{i,j} c_{i,j}$ with $b_{i,j} \in \mathfrak{b}$ and $c_{i,j} \in \mathfrak{c}$. Hence we have

$$x = \sum_{i=1}^{n} a_i d_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m_i} b_{i,j} c_{i,j} \right) = \sum_{i=1}^{n} \sum_{j=1}^{m_i} (a_i b_{i,j}) c_{i,j}.$$

Now $(a_i b_{i,j}) c_{i,j} \in (\mathfrak{a}\mathfrak{b})\mathfrak{c}$ for each i. Since ideals are closed under addition, we see that $x \in (\mathfrak{a}\mathfrak{b})\mathfrak{c}$. We have thus shown the inclusion"$\subset$". The argument for "$\supset$" is analogous.

(c) Using first (b) and then (a) shows that $(x) \cdot ((y) \cdot \mathfrak{a}) = ((x) \cdot (y)) \cdot \mathfrak{a} = (xy) \cdot \mathfrak{a}$.

8. Decide which of the following ideals of $\mathbb{Q}[X, Y, Z]$ are equal:

$$\begin{aligned} I_1 &:= (X, Y) & I_5 &:= (XZ, X - Y, X + Y) \\ I_2 &:= (X, Y, Z) & I_6 &:= (X^2 + Y^2, Z - Y^2, Z - X^2) \\ I_3 &:= (X^2, Y^2, Z) & I_7 &:= (XZ, Y^2 - 5X^2, X^2 - XZ) \\ I_4 &:= (XZ, X^2, Y^2) \end{aligned}$$

Solution: For each monomial M, the ideal (M) consists of those polynomials in which only those monomials occur that are divisible by M. For any monomials $M_1, \ldots, M_n$, $(M_1, \ldots, M_n)$ therefore consists of those polynomials in which only those monomials occur that are divisible by at least one of the M_i. Thus Z lies in the ideals I_2 and I_3, but not in I_1 or I_4. Furthermore, Y lies in the ideals I_1 and I_2, but not in I_3 or I_4. Therefore, the ideals I_1 to I_4 are all different.

Then I_5 contains the two elements

$$\begin{aligned} \tfrac{1}{2} \cdot \big((X + Y) + (X - Y) \big) &= X \quad \text{and} \\ \tfrac{1}{2} \cdot \big((X + Y) - (X - Y) \big) &= Y \end{aligned}$$

Conversely, since $X \pm Y$ are linear combinations of these elements, this ideal is equal to (XZ, X, Y). Here, XZ is already a multiple of X; we can therefore omit this generating end. Therefore, $I_5 = (X, Y) = I_1$.

We calculate analogously

$$\begin{aligned} \tfrac{1}{2} \cdot \big((X^2 + Y^2) + (Z - Y^2) + (Z - X^2) \big) &= Z \quad \text{and} \\ Z - (Z - X^2) &= X^2 \quad \text{and} \\ Z - (Z - Y^2) &= Y^2. \end{aligned}$$

Conversely, $X^2 + Y^2, Z - Y^2, Z - X^2$ are already linear combinations of Z, X^2, Y^2; thus the ideal I_6 is equal to I_3.

Finally, we calculate

$$\begin{aligned} XZ + (X^2 - XZ) &= X^2 \quad \text{and} \\ (Y^2 - 5X^2) + 5 \cdot X^2 &= Y^2. \end{aligned}$$

Conversely, $Y^2 - 5X^2$ and $X^2 - XZ$ are already linear combinations of XZ, X^2, Y^2; thus the ideal I_7 is equal to I_4.

9. For $\omega = e^{\frac{2\pi i}{3}}$ consider the ring $R := \mathbb{Z}[\omega] \subset \mathbb{C}$ with the *field norm*

$$N\colon R \to \mathbb{Z}_{\geqslant 0},\ a + b\omega \mapsto a^2 - ab + b^2.$$

(a) Show that the field norm N is multiplicative.

(b) Prove that R is a Euclidean ring with respect to N.

(c) Determine the group of units $R^\times$. [*Hint:* Use part (b).]

(d) Write $5 + \omega$ as a product of prime elements from R.

(e) Prove that each prime element of R divides exactly one prime number $p \in \mathbb{Z}$.

Solution:

(a) The field norm N satisfies $N(1) = 1$ and is multiplicative: for all $a = r + s\omega, b = u + v\omega \in R$, with $r, s, u, v \in \mathbb{Z}$, we have

$$\begin{aligned}
N(ab) &= N((r + s\omega)(u + v\omega)) \\
&= N(ru + (rv + su)\omega + sv\omega^2) \\
&= N((ru - sv) + (rv + su - sv)\omega) \\
&= (ru - sv)^2 - (ru - sv)(rv + su - sv) + (rv + su - sv)^2 \\
&= (r^2 - rs + s^2)(u^2 - uv + v^2) \\
&= N(a)N(b).
\end{aligned}$$

(b) Let $x, y \in R$ with $y \neq 0$. We can write $\frac{x}{y} = a + b\omega$ with $a, b \in \mathbb{Q}$. Choose $m, n \in \mathbb{Z}$ such that

$$|a - m| \leqslant \frac{1}{2} \quad \text{and} \quad |b - n| \leqslant \frac{1}{2}$$

and let $q := m + n\omega$ and $r := x - yq$. From our construction we obtain:

$$N\left(\frac{x}{y} - q\right) = (a - m)^2 - (a - m)(b - n) + (b - n)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

Then we have $x = yq + r$ with

$$N(r) = N(x - yq) = N(y)N\left(\frac{x}{y} - q\right) < N(y).$$

Thus R is a Euclidean ring for the function N.

(c) If $s \in R^\times$ is a unit, then also $s^{-1} \in R^\times$. Hence

$$N(s) \cdot N(s^{-1}) = N(ss^{-1}) = N(1) = 1.$$

On the other hand, to determine all the elements $s \in R$ with $N(s) = 1$, we can use the quadratic formula for the equation $x^2 - xy + y^2 - 1 = 0$ to obtain

$$\begin{aligned}
y &= \frac{1}{2}(x - \sqrt{4 - 3x^2}) \\
y &= \frac{1}{2}(\sqrt{4 - 3x^2} + x).
\end{aligned}$$

Considering possible integer solutions for the equations above, we obtain that $\pm 1, \pm\omega$ are the only elements $s \in R$ with $N(s) = 1$. Hence

$$s \in R^\times \iff N(s) = 1 \iff s \in \{\pm 1, \pm\omega, \pm(1+\omega)\}.$$

(d) Since $N(5\omega + 1) = 21$, we can write $5\omega + 1$ as a product of at most two elements $s, r \in R \backslash R^\times$ of norm 3 and 7. Since N is multiplicative, we have that r and s have to be irreducible. By trying out, we find that the element $N(1-\omega) = 3$ and $N(3+\omega) = 7$, and that there is a decomposition

$$5\omega + 1 = (1-\omega)(3+\omega) \cdot \omega,$$

where $\omega \in R^\times$ by part (c). The ring R is Euclidean, so it is also factorial, which means that irreducible elements are prime and the decomposition above is a product of prime elements.

(e) Let $a = r + s\omega \in R$ be prime. Since a is not a unit, we have $N(a) > 1$ since $N(a) = r^2 + s^2 - rs = \frac{1}{2}(r^2 + s^2 - 2rs) + \frac{1}{2}(r^2 + s^2) \geqslant 0$, so that $N(a)$ has a non-trivial decomposition into prime numbers $N(a) = p_1 \cdots p_k$. Note that $N(a) = N(r + s\omega)N(r + s\omega^2) = a \cdot \overline{a}$, so that a divides at least one prime number p_i, since a is prime.

Let us assume that a divides two different prime numbers p and q. Then we have that 1 is a $\mathbb{Z}$-linear combination of p and q and hence also a R-linear combination. Hence a divides the elements $1 \in R$, which is a contradiction.