DISCUSSION AND PROBLEM SESSION

1. Discussion and Problem session 1

1.1. Ring of functions.

(a) Is the set of continuous real valued functions on the interval $[0, 1]$ a ring under the point-wise addition and multiplication

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x)g(x)?$$

(b) How about the set of non-negative real valued continuous functions on the interval $[0, 1]$?

(c) Suppose $X$ is a non-empty set and $A$ is a ring. Is the set $\{f : X \to A\}$ of functions from $X$ to $A$ is a ring under the point-wise addition and multiplication

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x)?$$

1.2. Ring of polynomials.

(a) Let $f(x) \in (\mathbb{Z}_2 \times \mathbb{Z}_3)[x], f(x) := (1, 2)x + (0, 2)$ and $g(x) \in (\mathbb{Z}_2 \times \mathbb{Z}_3)[x], g(x) := (1, 0)x + (2, 2)$. Find $f(x)g(x)$.

(b) What is the caveat of viewing polynomials in $A[x]$ as functions from $A$ to $A$?

(c) Suppose $p$ is a prime. Find $(x + 1)^p$ in $\mathbb{Z}_p[x]$.

1.3. Certain subrings of complex numbers.

(a) Show that the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $i$ is

$$\{a + bi | a, b \in \mathbb{Q}\}.$$ 

(b) Show that the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{2}$ is

$$\{a + \sqrt{2}b | a, b \in \mathbb{Q}\}.$$ 

(c) Describe the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt[3]{2}$. 

2. Discussion and Problem session 2

2.1. Ring isomorphism, kernel, and image.

(a) Describe all ring isomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_n$.

(b) Notice that $A := \{(a, a) | a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$. Can $A$ be a kernel of a ring homomorphism from $\mathbb{Z} \times \mathbb{Z}$ to some other ring?

(c) Prove that the rings $\{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ and

$$\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \right\} | a, b \in \mathbb{Q}\}$$

are isomorphic.
(d) Prove that the rings $\mathbb{Z}_5 \times \mathbb{Z}_5$ and
\[
\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_5 \}
\]
are isomorphic. (This is more challenging. Do not do it in the first round.)

2.2. Scaler multiplication by integers in rings.

(a) Suppose $A$ is a unital commutative ring. Prove that for every $n \in \mathbb{Z}$, $a, b \in A$, we have
\[
(na) \cdot b = n(a \cdot b) = a \cdot (nb).
\]
Do you think this is because of the associative property or the distributive property?

(b) Suppose $A$ is a unital commutative ring. Prove that for every $m, n \in \mathbb{Z}$ and $a, b \in A$ we have
\[
(ma) \cdot (nb) = (mn)(a \cdot b)
\]

(c) Let $e : \mathbb{Z} \to A, e(k) := k1_A$ and $A := \mathbb{Z}_m \times \mathbb{Z}_n$ where $m, n \in \mathbb{Z}$ and $\gcd(m, n)$. Find $\ker e$ and $\operatorname{Im} e$.

2.3. The evaluation map.

(a) What is the kernel of the evaluation map $\phi_i : \mathbb{Q}[x] \to \mathbb{C}, \phi_i(f(x)) := f(i)$?

(b) What is the kernel of the evaluation map $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}, \phi_{\sqrt{2}}(f(x)) := f(\sqrt{2})$?

3. Discussion and Problem session 3

3.1. Evaluation map.

(a) Let $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation map $\phi_i(f(x)) = f(i)$. Prove that
\[
\mathbb{Q}[i] := \operatorname{Im} \phi_i = \{a_0 + a_1i \mid a_0, a_1 \in \mathbb{Q}\}.
\]

(b) Let $\phi_{\sqrt{3}} : \mathbb{Q}[x] \to \mathbb{C}$ be the evaluation map $\phi_{\sqrt{3}}(f(x)) = f(\sqrt{3})$. Prove that
\[
\mathbb{Q}[\sqrt{3}] := \operatorname{Im} \phi_{\sqrt{3}} = \{a_0 + a_1 \sqrt{3} + a_2 \sqrt{3}^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}.
\]

(c) Suppose $\alpha \in \mathbb{C}$ is a zero of $p(x) = x^3 - x - 1$. Let $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$ be the corresponding evaluation map. Describe $\mathbb{Q}[\alpha]$.

3.2. Units.

(a) Find $|\mathbb{Z}_p^\times|$ where $p$ is prime and $k$ is a positive integer.

(b) Find $|(\mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}})^\times|$, where $p_i$’s are prime.

(c) Prove the Fermat’s little theorem which states $a^p \equiv a \pmod{p}$ for every integer $a$ and every prime $p$.

(d) Find $\mathbb{Q}[x]^\times$.

3.3. Fields.

(a) Prove that $\mathbb{Q}[i]$ is a field.

(b) Prove that $\mathbb{Q}[\sqrt{2}]$ is a field.

(c) Prove that $F := \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \}$ is a field of order 9. Is $F$ isomorphic to $\mathbb{Z}_9$? Is $F$ isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$?
4.1. Kernel, image, and isomorphism.

(a) Suppose $F$ is a field and $f : F \to A$ is a ring homomorphism. Prove that either $f$ is injective or $f(x) = 0$ for every $x \in F$.

(b) Prove that $\mathbb{Q}[i]$ is not isomorphic to $\mathbb{Q}[\sqrt{2}]$.

(c) Suppose $A$ is a unital ring and $D$ is an integral domain. Suppose $f : A \to D$ is a ring homomorphism. Prove that either $f(1_A) = 1_D$ or $f(x) = 0$ for every $x \in A$. Does this statement hold if $D$ is not an integral domain?

4.2. Field of fractions.

(a) Prove that $\mathbb{Q}(\mathbb{Z}) \simeq \mathbb{Q}$.

(b) Suppose $F$ is a field. Prove that $\mathbb{Q}(F) \simeq F$.

(c) Suppose $F$ is a field of characteristic zero. Prove that $\mathbb{Q}$ can be embedded into $F$.

(d) Prove that $\mathbb{Q}(\mathbb{Z}[\sqrt{2}]) \simeq \mathbb{Q}[\sqrt{2}]$.

(e) Give an example of an infinite field of characteristic $p > 0$.

4.3. Ring of formal power series. (Additional related topic for more motivated students) Suppose $F$ is a field. Let $F[x]$ be the ring of formal power series with coefficients in $F$; that means

$$F[x] := \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in F \right\},$$

and we have

$$\left( \sum_{i=0}^{\infty} a_i x^i \right) + \left( \sum_{i=0}^{\infty} b_i x^i \right) := \sum_{i=0}^{\infty} (a_i + b_i) x^i \quad \text{and} \quad \left( \sum_{i=0}^{\infty} a_i x^i \right) \left( \sum_{i=0}^{\infty} b_i x^i \right) := \sum_{n=0}^{\infty} \left( \sum_{i=0}^{n} a_i b_{n-i} \right) x^n.$$

One can easily check that $(F[x], +, \cdot)$ is a ring. Similarly let

$$F(\langle x \rangle) := \left\{ \sum_{i=n}^{\infty} a_i x^i \mid n \in \mathbb{Z}, a_i \in F \right\}$$

and make this into a ring.

(a) Prove that $F[x]$ is an integral domain.

(b) Prove that $F(\langle x \rangle)$ is a field.

(c) Prove that $Q(F[x]) \simeq F(\langle x \rangle)$.

5. Discussion and Problem session 5

5.1. Ideals.

(a) Suppose $A$ is a unital commutative ring and $I, J \triangleleft A$. Let

$$I + J := \{ x + y \mid x \in I, y \in J \},$$

and

$$I \cdot J := \left\{ \sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{Z}^+, x_i, y_i \in I, y_i \in J \right\}.$$

Prove that $I + J$ and $I \cdot J$ are ideals of $A$. Is the set $\{ xy \mid x \in I, y \in J \}$ an ideal of $A$?

(b) Show that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer $n$. Deduce that all ideals of $\mathbb{Z}$ are principal.

(c) Prove that $\langle 2, x \rangle$ in $\mathbb{Z}[x]$ is not a principal ideal.
5.2. The first isomorphism theorem.

(a) Prove that \( \mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}_n[x] \).

(b) Prove that \( \mathbb{Q}[x]/\langle x^3 - 2 \rangle \simeq \mathbb{Q}[\sqrt[3]{2}] \) and moreover
\[
\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1 \sqrt[3]{2} + a_2 (\sqrt[3]{2})^2 | a_0, a_1, a_2 \in \mathbb{Q}\}.
\]

(c) Suppose \( p(x) \in \mathbb{Q}[x] \) has no zero in \( \mathbb{Q} \), \( \deg p = 3 \), and \( \alpha \in \mathbb{C} \) is a zero of \( p(x) \). Prove that
\[
\mathbb{Q}[x]/\langle p(x) \rangle \simeq \mathbb{Q}[\alpha],
\]
and moreover
\[
\mathbb{Q}[\alpha] = \{a_0 + a_1 \alpha + a_2 \alpha^2 | a_i \in \mathbb{Q}\}.
\]

6. Discussion and Problem session 6

6.1. The first isomorphism theorem. Since in the previous session we did not have time to go over the problems related to the first isomorphism theorem, I have included them here.

(a) Prove that \( \mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}_n[x] \).

(b) Prove that \( \mathbb{Q}[x]/\langle x^3 - 2 \rangle \simeq \mathbb{Q}[\sqrt[3]{2}] \) and moreover
\[
\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1 \sqrt[3]{2} + a_2 (\sqrt[3]{2})^2 | a_0, a_1, a_2 \in \mathbb{Q}\}.
\]

(c) Suppose \( p(x) \in \mathbb{Q}[x] \) has no zero in \( \mathbb{Q} \), \( \deg p = 3 \), and \( \alpha \in \mathbb{C} \) is a zero of \( p(x) \). Prove that
\[
\mathbb{Q}[x]/\langle p(x) \rangle \simeq \mathbb{Q}[\alpha],
\]
and moreover
\[
\mathbb{Q}[\alpha] = \{a_0 + a_1 \alpha + a_2 \alpha^2 | a_i \in \mathbb{Q}\}.
\]

(d) Prove that \( \mathbb{Z}[i]/\langle 2 + i \rangle \simeq \mathbb{Z}_5 \).

6.2. Polynomials.

(a) Find the quotient and the remainder of \( x^3 - x + 1 \) divided by \( x^2 - 1 \) in \( \mathbb{Q}[x] \).

(b) Let \( f(x, y) := x^4 + x^2 y^3 + xy + y^5 \). We can view \( f \) as an element of \( \mathbb{Q}[x][y] \) or as an element of \( \mathbb{Q}[y][x] \).
   1. View \( f \) as an element of \( \mathbb{Q}[x][y] \), and find \( \text{Ld}(f) \).
   2. View \( f \) as an element of \( \mathbb{Q}[y][x] \), and find \( \text{Ld}(f) \).

(c) Let \( f = x^3 + xy + y^2 \) and \( g = x^2 - y \). View \( f \) and \( g \) as elements of \( \mathbb{Q}[x][y] \), and find the remainder of \( f \) divided by \( g \).

(d) Suppose that \( A \) is a unital commutative ring and \( a_1, \ldots, a_n \) are nilpotent elements of \( A \) and \( a_0 \in A^\times \).
   1. Prove that \( a_1 x + a_2 x^2 + \cdots + a_n x^n \) is nilpotent.
   2. Prove that \( a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in A^\times \).
7. **Discussion and Problem session 7**

### 7.1. Quiz 1, version a.

1. Answer the following questions and briefly justify your answers.
   (a) (1 point) True or false. Every integral domain can be embedded into a field.
   (b) (2 point) Find $|\mathbb{Z}[x]|$.
   (c) (3 points) True or false. There is an integral domain $D$ such that
   
   $$1_D + \cdots + 1_D = 0 \quad \text{and} \quad 1_D + 1_D + 1_D \neq 0.$$  

   (d) (4 points) Find $|\mathbb{Z}_9 \times \mathbb{Z}_5|^9$.

2. (5 points) Prove that $\mathbb{Q}[x]/\langle x^2 - 3 \rangle \simeq \mathbb{Q}[\sqrt{3}]$ where $\mathbb{Q}[\sqrt{3}]$ is the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt{3}$.

3. (5 points) Suppose $p$ is a prime number and $f(x) \in \mathbb{Z}_p[x]$ is a polynomial of degree 3. Use the long division for polynomials to prove that $|\mathbb{Z}_p[x]/\langle f(x) \rangle| = p^3$.

4. (4 points) Suppose $m$ and $n$ are positive integers and $\gcd(m, n) = 1$. Let $e : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $e(k) := k(1)_m, (1)_n$.

   (a) (3 points) Find the kernel of $e$.
   (b) (4 points) Prove that $e$ is surjective.
   (c) (3 points) Prove that $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.

### 7.2. Quiz 1, version b.

1. Answer the following questions and briefly justify your answers.
   (a) (1 points) True or false. Every integral domain is a field.
   (b) (2 point) True or false. A field has exactly two ideals.
   (c) (3 points) Find the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}_7$.
   (d) (4 points) Find $|\mathbb{Z}_25 \times \mathbb{Z}_7|^8$.

2. Let’s recall that $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$.

   (a) (4 points) Prove that $\mathbb{Q}[x]/\langle x^2 + 1 \rangle \simeq \mathbb{Q}[i]$.
   (b) (2 points) Prove that $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$ is a field.

3. (4 points) Suppose $p$ is prime. Prove that $x^p^2 - x + 1$ has no zero in $\mathbb{Z}_p$.

4. (4 points) Suppose $\alpha \in \mathbb{C}$ is a zero of a polynomial $p(x) \in \mathbb{Q}[x]$ of degree 3. Use the long division for polynomials to prove that $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$

5. Let’s recall that $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

   (a) (2 points) Suppose $p$ is a prime and there is a ring homomorphism $f : \mathbb{Z}[i] \to \mathbb{Z}_p$ such that $f(1) = 1$. Prove that there is $x \in \mathbb{Z}_p$ such that $x^2 = -1$.
   (b) (4 points) Find a surjective ring homomorphism $f : \mathbb{Z}[i] \to \mathbb{Z}_{13}$ such that $3 - 2i \in \ker f$. (Notice that $8^2 + 1$ is a multiple of 13.)
8. Discussion and Problem session 8

8.1. Polynomials. (In the previous session we did not have time to go over these problems.)

1. Find the quotient and the remainder of \(x^3 - x + 1\) divided by \(x^2 - 1\) in \(\mathbb{Q}[x]\).
2. Let \(f(x, y) := x^4 + x^2y^3 + xy + y^2\). We can view \(f\) as an element of \((\mathbb{Q}[x])[y]\) or as an element of \((\mathbb{Q}[y])[x]\).
   1. View \(f\) as an element of \((\mathbb{Q}[x])[y]\), and find \(\text{Ld}(f)\).
   2. View \(f\) as an element of \((\mathbb{Q}[y])[x]\), and find \(\text{Ld}(f)\).
3. Let \(f = x^3 + xy + y^2\) and \(g = x^2 - y\). View \(f\) and \(g\) as elements of \((\mathbb{Q}[x])[y]\), and find the remainder of \(f\) divided by \(g\).
4. Suppose that \(A\) is a unital commutative ring and \(a_1, \ldots, a_n\) are nilpotent elements of \(A\) and \(a_0 \in A^\times\).
   1. Prove that \(a_1x + a_2x^2 + \cdots + a_n x^n\) is nilpotent.
   2. Prove that \(a_0 + a_1x + a_2x^2 + \cdots + a_n x^n \in A[x]^\times\).

8.2. Euclidean domains.

1. Prove that \(\mathbb{Z}[\sqrt{-2}]\) is a Euclidean domain and a PID.
2. Suppose \(F\) is a field. For an indeterminant \(x\), let

\[
F[x, x^{-1}] := \left\{ \sum_{i=-n}^{m} a_i x^i \mid a_i \in F \right\}.
\]

One can easily see that \(F[x, x^{-1}]\) with natural addition and multiplication is a ring. This is called the ring of \textit{Laurent polynomials}. Prove that \(F[x, x^{-1}]\) is a Euclidean domain.

(Hint. Every non-zero element of \(F[x, x^{-1}]\) can be uniquely written as \(x^{-n}f(x)\) for some non-negative integer \(n\) and polynomial \(f(x) \in F[x]\).)

8.3. Problems related to earlier topics.

1. Is there an integral that contains exactly 12 elements?
2. Suppose \(F\) is a field of characteristic \(p > 0\). Prove that \(F[x]/(x^p) \simeq F[x]/(x^p - 1)\).

9. Discussion and Problem session 9

9.1. Problems related to earlier topics. (In the previous session we did not have time to go over these problems.)

1. Suppose \(F\) is a field. For an indeterminant \(x\), let

\[
F[x, x^{-1}] := \left\{ \sum_{i=-n}^{m} a_i x^i \mid a_i \in F \right\}.
\]

One can easily see that \(F[x, x^{-1}]\) with natural addition and multiplication is a ring. This is called the ring of \textit{Laurent polynomials}. Prove that \(F[x, x^{-1}]\) is a Euclidean domain.

(Hint. Every non-zero element of \(F[x, x^{-1}]\) can be uniquely written as \(x^{-n}f(x)\) for some non-negative integer \(n\) and polynomial \(f(x) \in F[x]\).)
2. Is there an integral that contains exactly 12 elements?
3. Suppose \(F\) is a field of characteristic \(p > 0\). Prove that \(F[x]/(x^p) \simeq F[x]/(x^p - 1)\).

1. How many elements does $\mathbb{Z}[x]/(x^3 - x + 1)$ have?
2. Suppose $\alpha$ is a zero of $x^3 - x + 1 \in \mathbb{Q}[x]$. Find the minimal polynomial $m_{\alpha, \mathbb{Q}}(x)$.
3. Show that every element of $\mathbb{Q}[\alpha]$ can be uniquely written as $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbb{Q}$.
4. Find $(x^3 - x + 1, x^2 + 1) \subseteq \mathbb{Q}[x]$.
5. Suppose $\alpha \in \mathbb{C}$ is a zero of $x^3 - x + 1$. Is $(\alpha^2 + 1)^{-1} \in \mathbb{Q}[\alpha]$?
6. Can we show that $\mathbb{Q}[\alpha]$ is a field?

10. Discussion and Problem session 10

10.1. Minimal polynomial and elements of a quotient of a ring of polynomials. (In the previous session we did not have time to go over these problems.)

1. How many elements does $\mathbb{Z}[x]/(x^3 - x + 1)$ have?
2. Suppose $\alpha$ is a zero of $x^3 - x + 1 \in \mathbb{Q}[x]$. Find the minimal polynomial $m_{\alpha, \mathbb{Q}}(x)$.
3. Show that every element of $\mathbb{Q}[\alpha]$ can be uniquely written as $a_0 + a_1\alpha + a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbb{Q}$.
4. Find $(x^3 - x + 1, x^2 + 1) \subseteq \mathbb{Q}[x]$.
5. Suppose $\alpha \in \mathbb{C}$ is a zero of $x^3 - x + 1$. Is $(\alpha^2 + 1)^{-1} \in \mathbb{Q}[\alpha]$?
6. Can we show that $\mathbb{Q}[\alpha]$ is a field?

10.2. Irreducible elements.

1. Suppose $p = a^2 + b^2$ is prime for some integers $a$ and $b$. Prove that $a + ib$ is irreducible in $\mathbb{Z}[i]$ and $p$ is not irreducible in $\mathbb{Z}[i]$.
2. Suppose $p$ is a prime which cannot be written as $a^2 + b^2$ for some integers $a$ and $b$. Prove that $p$ is irreducible in $\mathbb{Z}[i]$.
3. Let $\omega := \frac{-1 + \sqrt{-3}}{2}$. Suppose $p = a^2 - ab + b^2$ is a prime for some integers $a$ and $b$. Prove that $a + b\omega$ is irreducible in $\mathbb{Z}[\omega]$ and $p$ is not irreducible in $\mathbb{Z}[\omega]$.
4. Suppose $p$ is a prime which cannot be written as $a^2 - ab + b^2$ for some integers $a$ and $b$. Prove that $p$ is irreducible in $\mathbb{Z}[\omega]$.

10.3. Maximal ideal.

1. Let $p := (p_1, \ldots, p_n) \in \mathbb{C}$ and $\phi_p(f(x_1, \ldots, x_n)) := f(p)$ be the evaluation map from the ring of multivariable polynomials $\mathbb{C}[x_1, \ldots, x_n]$ to $\mathbb{C}$. Prove that $\ker \phi_p$ is a maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$.
2. Suppose $I$ is a maximal ideal of a unital commutative ring $A$. Prove that if $ab \in I$, then either $a \in I$ or $b \in I$.
3. Suppose $D$ is a PID and $a \in D$ is irreducible. Prove that $a|bc$ implies that either $a|b$ or $a|c$.

11. Discussion and Problem session 11

11.1. Irreducible elements. (In the previous session we did not have time to go over these problems.)

1. Let $\omega := \frac{-1 + \sqrt{-3}}{2}$. Suppose $p = a^2 - ab + b^2$ is a prime for some integers $a$ and $b$. Prove that $a + b\omega$ is irreducible in $\mathbb{Z}[\omega]$ and $p$ is not irreducible in $\mathbb{Z}[\omega]$.
2. Suppose $p$ is a prime which cannot be written as $a^2 - ab + b^2$ for some integers $a$ and $b$. Prove that $p$ is irreducible in $\mathbb{Z}[\omega]$.
11.2. Maximal ideal. (Some of these problems have been mentioned in the previous session.)

1. Let \( p := (p_1, \ldots, p_n) \in \mathbb{C} \) and \( \phi_p(f(x_1, \ldots, x_n)) := f(p) \) be the evaluation map from the ring of multivariable polynomials \( \mathbb{C}[x_1, \ldots, x_n] \) to \( \mathbb{C} \). Prove that \( \ker \phi_p \) is a maximal ideal of \( \mathbb{C}[x_1, \ldots, x_n] \).

2. Suppose \( I \) is a maximal ideal of a unital commutative ring \( A \). Prove that if \( ab \in I \), then either \( a \in I \) or \( b \in I \).

3. Suppose \( D \) is a PID and \( a \in D \) is irreducible. Prove that \( a | bc \) implies that either \( a | b \) or \( a | c \).

4. There is a result in ring theory which states that every proper ideal is contained in a maximal ideal. Using this result prove that if \( M \) is the only maximal ideal of a unital commutative ring \( A \), then \( A^M = A \setminus M \).

5. Use the fundamental theorem of algebra which states that every non-constant polynomial \( f(x) \in \mathbb{C}[x] \) has a complex root to prove that an ideal \( I \) of \( \mathbb{C}[x] \) is maximal if and only if \( I = (x - a) \) for some \( a \in \mathbb{C} \).

6. (a) Use the fundamental theorem of algebra, to show that every non-constant polynomial \( f(x) \in \mathbb{C}[x] \) can be written as a product of degree one polynomials.

(b) Suppose \( E \) is a field extension of \( \mathbb{C} \). Prove that if \( \alpha \in E \) is algebraic over \( \mathbb{C} \), then \( \alpha \in \mathbb{C} \).

(c) Suppose \( M \) is a maximal ideal of \( \mathbb{C}[x_1, \ldots, x_n] \). Prove that \( \mathbb{C}[x_1, \ldots, x_n]/M \simeq \mathbb{C} \).

12. Discussion and Problem session 12


1. Show that a polynomial of degree \( n \) with coefficients in an integral domain does not have more than \( n \) distinct zero.

2. Find all primes \( p \) such that \( x + 2 \) is a factor of \( x^4 - x + 1 \) in \( \mathbb{Z}_p[x] \).

3. Show that \( x^5 + x^4 + x^3 + x^2 + x - 1 \) does not have a zero in \( \mathbb{Q} \).

4. Show that \( x^{125} - x^{25} + x^5 - x + 6 \) does not have a zero in \( \mathbb{Q} \).

5. Show that \( x^{125} - x^{25} + x^5 - x + 1 + 5f(x) \) for some \( f(x) \in \mathbb{Z}[x] \) with degree less than 125 does not have a zero in \( \mathbb{Q} \).

12.2. Irreducible polynomials.

1. Prove that \( x^3 - 3x^2 + 3x + 4 \) is irreducible in \( \mathbb{Q}[x] \).

2. We are told that the only monic degree 2 irreducible polynomials in \( \mathbb{Z}_3[x] \) are \( x^2 + 1, x^2 + x - 1, \text{ and } x^2 - x - 1 \). Prove that \( x^3 - x + 1 \) is irreducible in \( \mathbb{Z}_3[x] \).

3. Prove that \( x^5 + 2x + 4 \) is irreducible in \( \mathbb{Q}[x] \).

4. Let \( F := \mathbb{Z}_3[x]/(x^5 - x + 1) \).

(a) Prove that \( F \) is a field of order \( 3^5 \).

(b) Prove that \( X^5 - X + 1 \) has a zero in \( F \).

13. Discussion and Problem sessions 13

We had quiz.

14. Discussion and Problem session 14


1. Answer the following questions and briefly justify your answers.

(a) (2 point) Find all primes \( p \) such that \( x - 1 \) is a factor of \( x^5 - 2x^4 + 3x^3 + 5x^2 + 6 \) in \( \mathbb{Z}_p \).

(b) (3 points) True or false. \( \mathbb{Z}[x] \) is a PID.
2. (5 points) Determine whether \( f(x) := x^5 - 2x^4 + 5x^3 - x + 1 \) has a zero in \( \mathbb{Q} \). Justify your answer.

3. Recall that \( \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \).
   (a) (4 points) Prove that \( 5 + 2i \) is irreducible in \( \mathbb{Z}[i] \).
     (Hint: Think about \( N(a + bi) = |a + bi|^2 = a^2 + b^2 \).)
   (b) (4 points) Prove that \( \mathbb{Z}[i]/(5 + 2i) \) is a field.
   (c) (2 points) Prove that the characteristic of \( \mathbb{Z}[i]/(5 + 2i) \) is 29.

4. Suppose \( E \) is a field extension of \( \mathbb{Z}_3 \), and \( \alpha \in E \) is a zero of \( x^3 - x + 2 \).
   (a) (6 points) Prove that \( \mathbb{Z}_3[\alpha] \) is a field of order 27.
   (b) (2 points) Prove that \( \alpha^{26} = 1 \). (Hint: Think about \( (\mathbb{Z}_3[\alpha])^\times \).
   (c) (2 points) Prove that \( x^3 - x + 2 \) divides \( x^{26} - 1 \).

14.2. Quiz 2, version b.

1. (3 points) Suppose \( I \) is an ideal of a unital commutative ring \( A \) and \( A/I \) is a finite integral domain. Show that \( I \) is a maximal ideal.

2. (5 points) Suppose \( D \) is an integral domain, \( f, g \in D[x] \) are polynomials of degree at most \( n \), and \( a_1, \ldots, a_{n+1} \) are distinct elements of \( D \). Prove that if \( f(a_i) = g(a_i) \) for every \( i \), then \( f(x) = g(x) \).

3. (5 points) Determine whether \( f(x) := x^{2021} - x + 100 \) has a zero in \( \mathbb{Q} \). Justify your answer.

4. Suppose \( \alpha \in \mathbb{C} \) is a zero of \( x^3 - x + 1 \).
   (a) (3 points) Find the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \).
   (b) (4 points) Argue why \( (\alpha^2 + 1)^{-1} \) can be written as \( a_0 + a_1 \alpha + a_2 \alpha^2 \) for some \( a_i \in \mathbb{Q} \). (You are allowed to use all the results proved in the lectures after carefully stating them.)

5. Suppose \( D \) is an integral domain which is not a field and \( a \in D \).
   (a) (4 points) Prove that \( x - a \) is irreducible in \( D[x] \).
   (b) (4 points) Prove that \( D[x]/(x - a) \simeq D \).
   (c) (2 points) Prove that \( D[x] \) is not a PID.

15. Discussion and Problem sessions 15

15.1. Noetherian rings.

1. Prove that the ring of polynomials \( \mathbb{Q}[x_1, x_2, \ldots] \) with infinitely many indeterminants \( x_1, x_2, \ldots \) is not Noetherian.

2. Let \( A := \mathbb{Q}[x, xy, xy^2, \ldots] \subseteq \mathbb{Q}[x, y] \). Prove that \( A \) is not Noetherian.

15.2. Decomposition.

1. Suppose \( F \) is a field and \( f(x) \in F[x] \) is a monic positive degree polynomial.
   (a) Suppose \( f \) is irreducible. Let \( E := F[x]/(f) \). Prove that \( E \) is a field extension of \( F \).
   (b) Suppose \( f \) is irreducible in \( F[x] \). Prove that there is a field extension \( E \) of \( F \) which contains a zero of \( f \).
   (c) Prove that there is a field extension \( E' \) of \( F \) such that \( f(x) = \prod_{i=1}^{n}(x - \alpha_i) \) for some \( \alpha_i \)'s in \( E' \).

2. Suppose \( p \) is prime.
(a) For every prime $p$, there is a finite field $E$ such that

$$x^{p^n} - x = \prod_{i=1}^{p^n}(x - \alpha_i)$$

for some $\alpha_i \in E$.

(b) Let $F := \{ \alpha \in E \mid \alpha^{p^n} = \alpha \}$. Prove that $F$ is a finite field of order $p^n$.

16. **Discussion and Problem sessions** 16

16.1. **Decomposition.**

1. Suppose $p$ is prime.

   (a) For every prime $p$, there is a finite field $E$ extension of $\mathbb{Z}_p$ such that

   $$x^{p^n} - x = \prod_{i=1}^{p^n}(x - \alpha_i)$$

   for some $\alpha_i \in E$.

   (b) Let $F := \{ \alpha \in E \mid \alpha^{p^n} = \alpha \}$. Prove that $F$ is a finite field of order at most $p^n$.

   (c) Prove that $|F| = p^n$.

2. Suppose $D$ is a UFD, $p \in D$ is prime, and $f(x) := c_nx^n + \cdots + a_0 \in D[x]$ satisfies the following property:

   $$p \nmid c_n, p|c_{n-1}, \ldots, p|c_0, \text{ and } p^2 \nmid c_0.$$  

   Prove that $f(x)$ cannot be written as a product of two smaller degree polynomials in $D[x]$.

3. Prove that $x^n + yx^{n-1} + \cdots + yx + y$ is irreducible in $\mathbb{Z}[x,y]$.

4. Prove that $a_nx^n + \cdots + a_0 \in \mathbb{Q}[x]$ is irreducible if and only if $a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$ is irreducible.

5. Suppose $f(x) := a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ and for a prime $p$ we have

   $$p|a_0, p|a_1, \ldots, p|a_k, p \nmid a_{k+1}, \text{ and } p^2 \nmid a_0.$$  

   Prove that $f(x)$ has an irreducible factor in $\mathbb{Q}[x]$ that has degree greater than $k$.

6. Prove that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Q}[x]$.

7. decompose 2 as a product of irreducible elements in $\mathbb{Z}[i]$. How many distinct factors does it have?

17. **Discussion and Problem sessions** 17

17.1. **Decomposition.**

1. Suppose $D$ is a UFD, $p \in D$ is prime, and $f(x) := c_nx^n + \cdots + a_0 \in D[x]$ satisfies the following property:

   $$p \nmid c_n, p|c_{n-1}, \ldots, p|c_0, \text{ and } p^2 \nmid c_0.$$  

   Prove that $f(x)$ cannot be written as a product of two smaller degree polynomials in $D[x]$.

2. Prove that $x^n + yx^{n-1} + \cdots + yx + y$ is irreducible in $\mathbb{Z}[x,y]$.

3. Prove that $x^n + y^n - 1$ is irreducible in $\mathbb{C}[x,y]$.

4. Prove that $x^3 + 12x^2 + 18x + 6$ is irreducible in $(\mathbb{Z}[i])[x]$.

5. Prove that $a_nx^n + \cdots + a_0 \in \mathbb{Q}[x]$ is irreducible if and only if $a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$ is irreducible.

6. Suppose $f(x) := a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ and for a prime $p$ we have

   $$p|a_0, p|a_1, \ldots, p|a_k, p \nmid a_{k+1}, \text{ and } p^2 \nmid a_0.$$  

   Prove that $f(x)$ has an irreducible factor in $\mathbb{Q}[x]$ that has degree greater than $k$.

7. Prove that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Q}[x]$. 
8. decompose 2 as a product of irreducible elements in \( \mathbb{Z}[i] \). How many distinct factors does it have?

**17.2. UFD and PID.**

1. Suppose \( D \) is a PID. Prove that every non-zero prime ideal is maximal.
2. Prove that \( \mathbb{C}[x, y]/(x^n + y^n - 1) \) is an integral domain.
3. Suppose \( D \) is a UFD, and \( \langle a, b \rangle = \langle \gcd(a, b) \rangle \) for every \( a, b \in D \setminus \{0\} \).
   
   (a) Prove that every finitely generated ideal of \( D \) is principal.
   
   (b) For every non-zero non-unit element \( a \) of \( D \), \( \{ \langle d \rangle \mid d \mid a \} \) is a finite set.
   
   (c) Prove that \( D \) is a PID.
4. Suppose \( D \) is a UFD. Prove that \( D \) is a PID if and only if \( \langle a, b \rangle = \langle \gcd(a, b) \rangle \), for every \( a, b \in D \setminus \{0\} \).

**18. Discussion and Problem sessions 18**


1. (5 points) Suppose \( n \) is a positive odd integer. Prove that \( f(x) = (x - 2)(x - 4) \cdots (x - 2n) - 1 \in \mathbb{Q}[x] \) is irreducible.

2. (5 points) Suppose \( f, g \in \mathbb{Z}[x] \) are monic, \( p \) is prime, and \( c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x] \) is the modulo-\( p \) residue map. Prove that if \( \gcd(c_p(f), c_p(g)) = 1 \) in \( \mathbb{Z}_p[x] \), then \( \gcd(f, g) = 1 \) in \( \mathbb{Q}[x] \).

3. Suppose \( D \) is a PID and \( I = \langle p \rangle \) is a non-zero prime ideal of \( D \).
   
   (a) (5 points) Prove that \( p \) is an irreducible element of \( D \).
   
   (b) (3 points) Prove that \( I \) is a maximal ideal of \( D \).

4. Suppose \( p \) is a prime, \( a \in \mathbb{Z}_p^\times \), and \( f(x) := x^p - x + a \in \mathbb{Z}_p[x] \). Suppose \( E \) is a field extension of \( \mathbb{Z}_p \), and \( \alpha \in E \) is a zero of \( f(x) \). Notice that the characteristic of \( E \) is \( p \).
   
   (a) (3 points) Prove that \( x^p - x + a = (x - \alpha) \cdots (x - \alpha - (p - 1)) \) in \( E[x] \).
   
   (b) (5 points) Prove that \( x^p - x + a \in \mathbb{Z}_p[x] \) is irreducible.
   
   (c) (2 points) State the relevant results from the lectures or HW assignments and show that \( \mathbb{Z}_p[\alpha] \) is a finite field of order \( p^\ell \).
   
   (d) (2 points) Prove that \( \prod_{a \in \mathbb{Z}_p^\times} (x^p - x + a) \) divides \( x^{p^\ell} - x \).

18.2. Quiz 3, version b.

1. (5 points) Suppose \( p \) is prime. Prove that \( x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{Q}[x] \) is irreducible.

2. (5 points) Suppose every ideal of a unital commutative ring \( A \) is finitely generated. Prove that \( A \) is Noetherian.

3. Suppose \( A \) is a subring of \( B \), \( B \) is a unital commutative ring, \( 1_B \in A \), and \( I \) is an ideal of \( B \).
   
   (a) (3 points) Prove that \( f : A \to B/I, f(a) := a + I \) is a ring homomorphism and \( \ker f = I \cap A \).
   
   (b) (5 points) Prove that if \( I \) is a prime ideal of \( B \), then \( I \cap A \) is a prime ideal of \( A \).
   
   (c) (2 points) Provide an example where \( I \) is a maximal ideal of \( B \), but \( I \cap A \) is not a maximal ideal of \( A \).
4. Suppose $p$ is prime and $f(x) := (x^p - x + 1)^2 + p$.
   (a) (5 points) Suppose $f(x) = q(x)h(x)$ for some monic non-constant polynomials $q, h \in \mathbb{Z}[x]$. Prove that there are polynomial $q_1, h_1 \in \mathbb{Z}[x]$ such that
   
   $q(x) = x^p - x + 1 + p \cdot q_1(x)$, and $h(x) = x^p - x + 1 + p \cdot h_1(x)$.
   
   (You are allowed to use a relevant result from HW assignment after you carefully state it.)

   (b) (3 points) Suppose $q_1$ and $h_1$ are as in the previous part. Prove that
   
   $(x^p - x + 1)(q_1 + h_1) \equiv 1 \pmod{p}$
   
   and discuss why this is a contradiction.

   (c) (2 points) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

19. Discussion and Problem sessions 19

19.1. Decomposition.

1. Prove that $x^n + yx^{n-1} + \cdots + yx + y$ is irreducible in $\mathbb{Z}[x, y]$. (Use Eisenstein’s criterion for UFDs.)

2. Prove that $x^n + y^n - 1$ is irreducible in $\mathbb{C}[x, y]$.

3. Prove that $x^n + 12x^2 + 18x + 6$ is irreducible in $(\mathbb{Z}[i])[x]$.

4. Prove that $a_nx^n + \cdots + a_0 \in \mathbb{Q}[x]$ is irreducible if and only if $a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$ is irreducible.

5. Suppose $f(x) := a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ and for a prime $p$ we have
   
   $p|a_0, p|a_1, \ldots, p|a_k, p \nmid a_{k+1}$, and $p^2 \nmid a_0$.

   Prove that $f(x)$ has an irreducible factor in $\mathbb{Q}[x]$ that has degree greater than $k$.

6. Prove that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Q}[x]$.

7. Decompose 2 as a product of irreducible elements in $\mathbb{Z}[i]$. How many distinct factors does it have?

8. Decompose 30 into prime factors in $\mathbb{Z}[i]$.

19.2. UFD and PID.

1. Suppose $D$ is a PID. Prove that every non-zero prime ideal is maximal.

2. Prove that $\mathbb{C}[x, y]/(x^n + y^n - 1)$ is an integral domain.

3. Suppose $D$ is a UFD, and $(a, b) = (\gcd(a, b))$ for every $a, b \in D \setminus \{0\}$.
   
   (a) Prove that every finitely generated ideal of $D$ is principal.

   (b) For every non-zero non-unit element $a$ of $D$, $\{d \mid d|a\}$ is a finite set.

   (c) Prove that $D$ is a PID.

4. Suppose $D$ is a UFD. Prove that $D$ is a PID if and only if $(a, b) = (\gcd(a, b))$, for every $a, b \in D \setminus \{0\}$.

20. Discussion and Problem sessions 20

20.1. Decomposition.

1. Suppose $f(x) := a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ and for a prime $p$ we have
   
   $p|a_0, p|a_1, \ldots, p|a_k, p \nmid a_{k+1}$, and $p^2 \nmid a_0$.

   Prove that $f(x)$ has an irreducible factor in $\mathbb{Q}[x]$ that has degree greater than $k$.

2. Prove that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Q}[x]$.

3. Decompose 2 as a product of irreducible elements in $\mathbb{Z}[i]$. How many distinct factors does it have?

4. Decompose 30 into prime factors in $\mathbb{Z}[i]$.
20.2. Splitting field.
1. Find a splitting field of \( x^p - 1 \) over \( \mathbb{Z}_p \).
2. Find a splitting field of \( x^3 - 1 \) over \( \mathbb{Q} \).
3. Suppose \( p \) is prime, and let \( E \) be a splitting field of \( x^p - 2 \) over \( \mathbb{Q} \). Find as many isomorphisms as you can from \( E \) to \( E \).

21. Discussion and Problem sessions 21

1. Find a splitting field of \( x^p - 1 \) over \( \mathbb{Z}_p \).
2. Find a splitting field of \( x^3 - 1 \) over \( \mathbb{Q} \).
3. Suppose \( F \) is a finite field of order \( p^n \) where \( p \) is prime. Find as many isomorphisms as you can from \( F \) to \( F \). (Hint: think about the Frobenious map \( \sigma : F \rightarrow F, \sigma(a) := a^p \).)
4. Suppose \( E \) is a field extension of \( F \), \( f(x) \in F[x] \), and \( \alpha \in E \) is a zero of \( f \). Suppose \( \theta : E \rightarrow E \) is an isomorphism such that \( \theta(c) = c \) for every \( c \in F \). Prove that \( \theta(\alpha) \) is a zero of \( f \).
5. Suppose \( \alpha \) is a positive integer, and let \( E \) be a splitting field of \( x^\alpha - 1 \) over \( \mathbb{Q} \). Find as many isomorphisms as you can from \( E \) to \( E \).
6. Suppose \( p \) is prime, and let \( E \) be a splitting field of \( x^p - 2 \) over \( \mathbb{Q} \). Find as many isomorphisms as you can from \( E \) to \( E \).
7. Suppose \( E \) is a splitting field of \( f \in F[x] \) and \( f \) is irreducible and has \( n \) distinct zeros. Argue that there are at least \( n \) isomorphisms from \( E \) to \( E \).

22. Discussion and Problem sessions 22

22.1. Splitting field.
1. Suppose \( p \) is prime, and let \( E \) be a splitting field of \( x^p - 2 \) over \( \mathbb{Q} \). Find as many isomorphisms as you can from \( E \) to \( E \).
2. Suppose \( E \) is a splitting field of \( f \in F[x] \) and \( f \) is irreducible and has \( n \) distinct zeros. Argue that there are at least \( n \) isomorphisms from \( E \) to \( E \).

22.2. Finite fields.
1. Suppose \( m \) and \( n \) are positive integers and \( p \) is prime.
   (a) Prove that \( p^m - 1 | p^n - 1 \) if and only if \( m | n \).
   (b) Suppose \( m | n \). Prove that \( x^{p^m} - x \) divides \( x^{p^n} - x \) in \( \mathbb{Z}_p[x] \).
   (c) Prove that \( \mathbb{F}_{p^m} \) can be embedded into \( \mathbb{F}_{p^n} \) if and only if \( m | n \).
2. Suppose \( \mathbb{F}_{p^m}^\alpha \) is generated by \( \alpha \). Prove that \( m \alpha, \mathbb{Z}_p(x) \) has degree \( n \).
3. Prove that for every positive integer \( n \) there is an irreducible polynomial of degree \( n \) in \( \mathbb{Z}_p[x] \).
4. Let \( \text{Irr}_p(d) := \{ f(x) \in \mathbb{Z}_p[x] \mid \deg f = d, f \text{ is irreducible in } \mathbb{Z}_p[x] \} \).
   (a) Prove that \( f \) is an irreducible factor of \( x^{p^n} - x \) if and only if \( \deg f | n \).
   (b) Prove that \( x^{p^n} - x = \prod_{d|n} \prod_{f \in \text{Irr}_p(d)} f(x) \).
5. Let \( \text{Aut}(\mathbb{F}_{p^n}) := \{ \theta : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n} \mid \theta \text{ is an isomorphism} \} \). Prove that \( |\text{Aut}(\mathbb{F}_{p^n})| = n \).

23. Discussion and Problem sessions 23

For a field extension \( E \) of \( F \), we let \( \text{Aut}_F(E) \) be the set of all \( F \)-isomorphisms from \( E \) to \( E \).
23.1. **Group of automorphisms.**

1. Justify why \( \text{Aut}_F(E), \sigma \) is a group.
2. Prove that \( \text{Aut}_E(F_p) \) is a cyclic group of order \( n \) which is generated by the Frobenius map \( \sigma : F_p \rightarrow F_p^n, \sigma(a) := a^p \).
3. Suppose \( n \) is a positive integer.
   (a) Suppose, for some integer \( a \), \( p \) is a prime factor of \( \Phi_n(a) \) which does not divide \( n \). Prove that \( p \equiv 1 \pmod{n} \) and \( \gcd(p, a) = 1 \). (Hint: Use Problem 4(b) and show that \( E_{n,p} = \mathbb{Z}_p \). Then use Problem 4(c).)
   (b) Prove that there are infinitely many primes in the arithmetic progression \( \{nk + 1\}_{k=1}^\infty \). (Hint: suppose \( p_1, \ldots, p_k \) are the only primes in this arithmetic progression. Since \( \Phi_n(np_1 \cdots p_k x) \) is not a constant polynomial, \( \Phi_n(np_1 \cdots p_k a) \neq \pm 1, 0 \) for some integer \( a \). Hence there is a prime factor \( p \) of \( \Phi_n(np_1 \cdots p_k a) \). Use Part (a) to deduce that \( p \) is different from \( p_i \)'s and \( p \equiv 1 \pmod{n} \).
4. Suppose \( G \) is a finite subgroup of \( \text{Aut}_E(E) \). Let
   \[ E^G := \{ a \in E \mid \forall \theta \in G, \theta(a) = a \}. \]
   (a) Prove that \( E^G \) is a subfield of \( E \).
   (b) For \( \alpha \in E \), let \( O_{\alpha,G} := \{ \theta(\alpha) \mid \theta \in G \} \),
       \[ p_{G,\alpha}(x) = \prod_{\alpha' \in O_{\alpha,G}} (x - \alpha'). \]
       Prove that \( p_{G,\alpha}(x) \in E^G[x] \) and \( \alpha \) is a zero of \( p_{G,\alpha}(x) \).
   (c) Prove that \( m_{\alpha,E^G}(x) = p_{G,\alpha}(x) \).

24. **Discussion and Problem sessions 24**

For a field extension \( E \) of \( F \), we let \( \text{Aut}_F(E) \) be the set of all \( F \)-isomorphisms from \( E \) to \( E \).

24.1. **Group of automorphisms.**

1. Suppose \( n \) is a positive integer.
   (a) Suppose, for some integer \( a \), \( p \) is a prime factor of \( \Phi_n(a) \) which does not divide \( n \). Prove that \( p \equiv 1 \pmod{n} \) and \( \gcd(p, a) = 1 \). (Hint: Use Problem 4(b) and show that \( E_{n,p} = \mathbb{Z}_p \). Then use Problem 4(c).)
   (b) Prove that there are infinitely many primes in the arithmetic progression \( \{nk + 1\}_{k=1}^\infty \). (Hint: suppose \( p_1, \ldots, p_k \) are the only primes in this arithmetic progression. Since \( \Phi_n(np_1 \cdots p_k x) \) is not a constant polynomial, \( \Phi_n(np_1 \cdots p_k a) \neq \pm 1, 0 \) for some integer \( a \). Hence there is a prime factor \( p \) of \( \Phi_n(np_1 \cdots p_k a) \). Use Part (a) to deduce that \( p \) is different from \( p_i \)'s and \( p \equiv 1 \pmod{n} \).
2. Suppose \( G \) is a finite subgroup of \( \text{Aut}_F(E) \). Let
   \[ E^G := \{ a \in E \mid \forall \theta \in G, \theta(a) = a \}. \]
   (a) Prove that \( E^G \) is a subfield of \( E \).
   (b) For \( \alpha \in E \), let \( O_{\alpha,G} := \{ \theta(\alpha) \mid \theta \in G \} \), and
       \[ p_{G,\alpha}(x) = \prod_{\alpha' \in O_{\alpha,G}} (x - \alpha'). \]
       Prove that \( p_{G,\alpha}(x) \in E^G[x] \) and \( \alpha \) is a zero of \( p_{G,\alpha}(x) \).
   (c) Prove that \( m_{\alpha,E^G}(x) = p_{G,\alpha}(x) \).
   (d) Prove that \( E \) is a normal extension of \( E^G \), and for every \( \alpha \in E \), \( \gcd(m_{\alpha,E^G}, m'_{\alpha,E^G}) = 1 \).
   (e) Prove that \( \text{Aut}_{E^G}(E) = G \).
For a field extension $E$ of $F$, we let $\text{Aut}_F(E)$ be the set of all $F$-isomorphims from $E$ to $E$.

25.1. Group of automorphisms.

1. Suppose $G$ is a finite subgroup of $\text{Aut}_F(E)$. Let

$$E^G := \{ a \in E \mid \forall \theta \in G, \theta(a) = a \}.$$

(a) Prove that $E^G$ is a subfield of $E$.

(b) For $\alpha \in E$, let $O_{\alpha,G} := \{ \theta(\alpha) \mid \theta \in G \}$, and

$$p_{G,\alpha}(x) = \prod_{\alpha' \in O_{\alpha,G}} (x - \alpha').$$

Prove that $p_{G,\alpha}(x) \in E^G[x]$ and $\alpha$ is a zero of $p_{G,\alpha}(x)$.

(c) Prove that $m_{\alpha,EG}(x) = p_{G,\alpha}(x)$.

(d) Prove that $E$ is a normal extension of $E^G$, and for every $\alpha \in E$, $\gcd(m_{\alpha,EG},m'_{\alpha,EG}) = 1$.

2. Suppose $p$ is prime and $\zeta_p = e^{2\pi i/p}$. Prove that

$$\text{Aut}_Q(Q[\zeta_p, \sqrt[p]{2}]) \simeq \left\{ \begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix} \mid i \in \mathbb{Z}_p^\times, j \in \mathbb{Z}_p \right\}.$$

3. Suppose $m|n$. Let $\sigma : F_{p^n} \to F_{p^n}, \sigma(a) := a^p$. Prove that the fixed points of $\sigma^m$ is a field of order $p^m$. Identify this field with $F_{p^m}$. Prove that $\text{Aut}_{\sigma^m}(F_{p^n})$ is a cyclic group of order $n/m$ which is generated by $\sigma^m$.

25.2. Normal extensions.


2. Can $\mathbb{Q}[\sqrt[4]{3}]$ be a normal extension of $\mathbb{Q}$ if $n > 2$?

3. Suppose $x^n - 1$ has $n$ zeros in a field $F$. Prove that $F[\sqrt[n]{a}]$ is a normal extension of $F$ for every $a \in F$. Prove that $\text{Aut}_F(F[\sqrt[n]{a}])$ is a cyclic group.