Midterm Exam

Friday, October 18, 2019

No books, notes or calculators

Problem 1.
Define the following terms. Some of them may have several equivalent definitions, in this case give only one definition.

(a) stem field,
Let K be a field, and $f \in K[x]$ an irreducible polynomial. The ring $L = K[x]/(f)$ is a field, together with a distinguished root $\overline{x} = x + (f)$ of f. The pair $(L, \overline{x})$ is called the **stem field** of f.

(b) splitting field,
Let K be a field, and $f \in K[x]$ a polynomial. A field extension L of K is called a **splitting field** of f, if f splits into linear factors in $L[x]$, and L is generated as a field extension of K by the roots of f in L.

(c) transcendental element,
Let L/K be a field extension. The element $\alpha \in L$ is **transcendental** over K, if there does not exist any non-zero polynomial $f \in K[x]$, such that $f(\alpha) = 0$.

(d) finite field extension.
A field extension L/K is **finite** if the dimension of L as a K-vector space is finite.

Problem 2.
Carefully state the following results:

(a) the Eisenstein irreducibility criterion,
Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. If there exists a prime number p, such that p divides all coefficients of f, but not the leading coefficient, and p^2 does not divide the constant coefficient, then f is irreducible in $\mathbb{Q}[x]$.

(b) a theorem that ensures that the number of K-morphisms $L \to L$ is equal to $|L : K|$. (Here $K \subset L$ is a field extension.)
Let L/K be a splitting field of a separable polynomial in $K[x]$. Then $\#\operatorname{Aut}(L/K) = |L : K|$.

Problem 3.
Give examples of the following phenomena (without proofs):

(a) a field extension of degree 203,
The stem field of any irreducible polynomial of degree 203 will do. For example $x^{203} - 15$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein. So the stem field $\mathbb{Q}(\sqrt[203]{15})$ of this polynomial is an extension of $\mathbb{Q}$ of degree 203.

(b) a polynomial whose stem field is not a splitting field of the polynomial.
It was shown in class that $x^3 - 2 \in \mathbb{Q}[x]$ has this property.

(c) an extension of $\mathbb{Q}(\sqrt{2})$ of degree 3.
The stem field of any irreducible polynomial of degree 3 in $\mathbb{Q}(\sqrt{2})[x]$ will do. One checks that $x^3 - 2$ has no root in $\mathbb{Q}(\sqrt{2})$, so it works.

(d) a field K, and a polynomial $f \in K[x]$, such that f has no root in K, and all roots of f in its splitting field coincide.
We need an inseparable polynomial. This requires a non-perfect field. The simplest non-perfect field is $\mathbb{F}_p(t)$, the field of rational functions in one variable over the finite field with p elements, p a prime number. The polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is irreducible, hence it has no roots, and all its roots in a splitting field coincide.

Give proofs:

Problem 4.

(a) How many $\mathbb{Q}$-morphisms $\mathbb{Q}(\sqrt[3]{3}) \longrightarrow \mathbb{C}$ are there?
The polynomial $x^3 - 3 \in \mathbb{Q}[x]$ is irreducible. So $\mathbb{Q}(\sqrt[3]{3})$ is the stem field of this polynomial. By the universal mapping property of the stem field, there are just as many $\mathbb{Q}$-morphisms $\mathbb{Q}(\sqrt[3]{3}) \longrightarrow \mathbb{C}$ as there are roots of $x^3 - 3$ in $\mathbb{C}$. The answer is 3.

(b) How many $\mathbb{Q}$-morphisms $\mathbb{Q}(\sqrt[3]{3}) \longrightarrow \mathbb{Q}(\sqrt[3]{3})$ are there?
There is only one root of $x^3 - 3$ in $\mathbb{Q}(\sqrt[3]{3})$. (To see this, we can be concrete by choosing the unique positive real cube root of 3 for $\sqrt[3]{3}$. Then the field $\mathbb{Q}(\sqrt[3]{3})$ is contained in $\mathbb{R}$, but the two other roots of $x^3 - 3$ in $\mathbb{C}$ are not real.) So there is only one such morphism.

Problem 5.

(a) Find the degree of the splitting field of the polynomial $x^5 - 1$ over $\mathbb{Q}$.
The polynomial $x^5 - 1$ has five complex roots, $1, \zeta, \zeta^2, \zeta^{-1}\zeta^{-2}$, where $\zeta = e^{2\pi i/5}$. We also have $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$, and since 5 if prime, $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible (this was shown in class). Uniqueness of roots of polynomials proves that in $\mathbb{C}[x]$ we have $x^4 + x^3 + x^2 + x + 1 = (x-\zeta)(x-\zeta^2)(x-\zeta^{-1})(x-\zeta^{-2})$. This proves that $\mathbb{Q}(\zeta)$ is the stem field of ζ over $\mathbb{Q}$, and that $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 4$. But now $\zeta^2, \zeta^{-1}, \zeta^{-2} \in \mathbb{Q}(\zeta)$, so the minimal polynomial of ζ splits completely over $\mathbb{Q}(\zeta)$. So $\mathbb{Q}(\zeta)$ is a splitting field for $x^4 + x^3 + x^2 + x + 1$, and also for $x^5 - 1$. The answer is 4.

(b) Find the degree of the splitting field of the polynomial $x^6 - 8$ over $\mathbb{Q}$.
The roots of the polynomial $x^6 - 8$ in $\mathbb{C}$ are $\omega^i\sqrt{2}$, for $i = 1, \ldots, 6$, where $\omega = e^{2\pi i/6} = \cos(60^\circ) + i\sin(60^\circ) = \frac{1+i\sqrt{3}}{2}$. A splitting field of $x^6 - 8 \in \mathbb{Q}[x]$ is therefore $\mathbb{Q}(\omega, \sqrt{2})$. (All roots are contained in this field, and the field is generated by the roots $\sqrt{2}$ and $\sqrt{2}\omega$.) We consider the iterated extension

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\omega, \sqrt{2})$. Each of these is of degree 2. This first, because $\sqrt{2}$ is not rational, but satisfies a degree 2 polynomial with coefficients in $\mathbb{Q}$, the second, because ω is not real, but satisfies a degree 2 polynomial with rational coefficients. So the total extension has degree 4. The answer is, again, 4.

Problem 6.

Prove that there exists a field with 27 elements, but there does not exist any field with 28 elements.

Find a polynomial of degree 3 in $\mathbb{F}_3[x]$ which is irreducible. For example $x^3 - x + 1$ works, because it has no roots in $\mathbb{F}_3$. Then the stem field of this polynomial is an extension of $\mathbb{F}_q$ of degree 3. It has $3^3 = 27$ elements.

Every finite field is a finite extension of its prime field. If the degree of this extension is n, then the field has p^n elements. So the number of elements of a finite field is necessarily a prime power. 28 is not a prime power.