6.3.12

Suppose that $\mathbb{F}_p$ is the finite field with a prime number p of elements. Supposte that A and B are non-squares in $\mathbb{F}_p$. Show that $F_p[\sqrt{A}] \simeq F_p[\sqrt{B}]$.

Solution:

Since AS, B are non-squares, they are non-zero. From last week, we know that $\mathbb{F}_p^*$ is cyclic, with generator W. A and B being non-squares is equivalent to $A = W^m$ and $B = W^n$, where m, n are odd integers. Therefore, $\frac{A}{B} = W^{m-n}$ is an even power of W, and therefore a square. So $A = C^2 B$, where $C = W^{\frac{m-n}{2}}$. Equipped with this fact, we can prove the main statement. In $\mathbb{F}_p[\sqrt{B}]$, we have an element $C\sqrt{B}$ such that

$$(C\sqrt{B})^2 = C^2 B = A$$

so this element is a square root of A. Hence $\mathbb{F}_p[\sqrt{B}]$ contains a subfield isomorphic to $\mathbb{F}_p[\sqrt{A}]$. Since for any element in $\mathbb{F}_p[\sqrt{B}]$ we can write it as:

$$x + y\sqrt{B} = x + yC^{-1}C\sqrt{B} = yC^{-1}\sqrt{A}$$

the subfield of $\mathbb{F}_p[\sqrt{B}]$ in question is in fact the whole field $\mathbb{F}_p[\sqrt{B}]$

6.3.13

Assume p is prime.

a) Show that there are $\frac{p-1}{2}$ irreducible polynomials of the form

$$f(x) = x^2 - \ in\mathbb{Z}_p[x]$$

b) Show that for every prime p, there exists a field with p^2 elements.

Solution:

We will assume that p is an odd prime, so the question makes sense. For the prime 2, there are 0 irreducible polynomials of this form, and not $\frac{1}{2}$, contradicting the statement of the exercise.

a) The polynomial $f(x)$ is irreducible if and only if b is not a square. Since b is in the cyclic group $\mathbb{F}_p^*$, with generator a, b is not a square if and only if it is an odd power of a. To find the number of such powers, we count the number of odd integers less than or equal to the order of $a = p - 1$, which is an even number, to get that there are $\frac{p-1}{2}$ non-square b, and therefore equally many irreducible polynomials of the desired form.

b) Since there is a polynomial $x^2 - b$, which is irreducible, the quotient $\mathbb{F}_p[x]/(x^2 - b) \simeq \mathbb{F}_p[\sqrt{b}]$ is a field with the desired number of elements.

Bonus question: Is there a field with 4 elements?

6.4.5

What is the field of fractions of $\mathbb{Z}_5$?

Solution:

The field of fractions is defined as the equivalence classes of pairs $\frac{a}{b}$ with $a \in Z_5, b \in Z_5^*$ and equivalence relation

$$\frac{a}{b} \sim \frac{c}{d} \text{ iff } ad = bc$$

We will prove that the field of fractions of $\mathbb{Z}_5$ is equal to $\mathbb{Z}_5$ by proving that each of the equivalence classes has a unique representative of the form $\frac{a}{1}$ for some a. Let $\frac{a}{b}$ be a fraction. Since $\mathbb{Z}_5$ is a field, we can find a multiplicative inverse $b^{-1} \in \mathbb{Z}_5$. We check that $\frac{a}{b} \simeq \frac{b^{-1}a}{1}$, where $b^{-1}a \in \mathbb{Z}_5$, so we have our represention. The representative is unique, since if $\frac{a}{1} \sim \frac{b}{1}$, the equivalence relation states that $a = b$. It follows from the rules for adding and multiplying fractions that $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}$ and $\frac{a}{1}\frac{b}{1} = \frac{ab}{1}$, which completes the proof that the fraction field of $\mathbb{Z}_5$ is $\mathbb{Z}_5$ itself.

6.4.6

Show that the field of fractions of an integral domain D is unique up to (unique) isomorphism.

Solution:

Assume $F\colon D \to D'$ is an isomorphism of integral domains, with fractions field K, K' respectively. Then $G\colon K \to K'$ defined by $G(\frac{a}{b}) = \frac{F(a)}{F(b)}$ is an isomorphism. Checking that G is a field homomorphism is straightforward:

$$G(\frac{a}{b} + \frac{c}{d}) = G(\frac{ad+bc}{bd}) = \frac{F(ad+bc)}{F(bd)} = \frac{F(a)}{F(b)} + \frac{F(c)}{F(d)}$$

$$G(\frac{a}{b}\frac{c}{d}) = G(\frac{ac}{bd}) = \frac{F(ab)}{F(cd)} = \frac{F(a)}{F(b)}\frac{F(c)}{F(d)}$$

G is surjective, since for any $\frac{a'}{b'} \in K'$, there exists $a \in D, b \in D^*$ such that $F(a) = a', F(b) = b'$, and therefore $G(\frac{a}{b}) = \frac{a'}{b'}$. Finally G is injective since $G(\frac{a}{b} = 0)$, then $F(a) = 0$, so since F is an isomorphism, $F(a) = 0$.

(We can recover F from G by restricting G to the subring of elements of the form $\frac{a}{1}$, which is isomorphic to D. Hence, for any two fields of fractions for a single integral domain D, there is a unique isomorphisms of the fields of fractions that restricts to the identity isomorphism of the subring of elements of the form $\frac{a}{1}$)

6.4.11

Consider the integral domain $\mathbb{Z}[\sqrt{5}]$. What is the field of fractions for $\mathbb{Z}[\sqrt{5}]$?

Solution:

The field $\mathbb{Q}[\sqrt{5}]$ is clearly a subfield of the field of fractions of $\mathbb{Z}[\sqrt{5}]$. We will show that the field of fractions is in fact $\mathbb{Q}[\sqrt{5}]$ We have the following equivalence of fractions:

$$\frac{a+b\sqrt{5}}{c+d\sqrt{5}} = \frac{(a+b\sqrt{5})(c-d\sqrt{5})}{(c+d\sqrt{5})(cd\sqrt{5})} = \frac{ac-5bd+(bd-ad)\sqrt{5}}{c^2-5d^2}$$

where the rightmost fraction is always defined since 5 is not a square, hence $c^2 - 5d^2$ is never zero. On the other hand, the rightmost fraction can be rewritten as

$$\frac{ac - 5bd}{c^2 - 5d^2} + \frac{bd - ad}{c^2 - 5d^2}\sqrt{5}$$

which is an element of $\mathbb{Q}[\sqrt{5}]$.

7.4.5

Is $x^4 + 1$ irreducible over $\mathbb{F}_3$?

Solution:

There are three elements of $\mathbb{F}_3$, namely $\{-1, 0, 1\}$. We check that no fourth power is equal to -1. So the polynomial has no degree 1 factors. There are three monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$, $x^2 + 1$, $x^2 + x - 1$ and $x^2 - x - 1$. We can compute that:

$$(x^2 + x - 1)(x^2 - x - 1) = x^4 - 3x^2 + 1 = x^4 + 1$$

so the polynomial is not irreducible.

7.4.6

Is $x^4 + 1$ irreducible over $\mathbb{F}_5$?

Solution:

If i is a square root of -1, we have in general:

$$(x^2 + i)(x^2 - i) = x^4 + 1$$

In $\mathbb{Z}_5$, 2 is a square root of -1, so:

$$x^4 + 1 = (x^2 + 2)(x^2 - 2)$$

7.4.7

Show that if K is an extension field of F and there is a transcendental element $a \in K$ over F, then K is an infinite-dimensional vector space over F. In fact, show that $F(a)$ is isomorphic to the field of fractions of the polynomial ring $F[x]$. This is a case in which $F(a) \neq F[a]$.

Solution:

Consider the homomorphism $f\colon F[x] \to K$ defined by $x \mapsto a$. The image of f is $F[a]$. Furthermore f must be injective, since otherwise any element in the kernel of would prove that a is algebraic. So $F[a]$ is isomorphic to $F[x]$, and therefore $F(a)$ is isomorphic to $F(x)$. To prove the main statement of the exercise, consider the elements $1, a, a^2, a^3, \dots \in K$. These are all distinct, since $F(a)$ is isomorphic to $F(x)$, and must be linearly independent over F, since otherwise a non-trivial linear dependence would prove that a is algebraic.

7.4.8

Suppose F is a finite field of characteristic p. Show that every element of F is algebraic over $\mathbb{F}_p$.

Solution:

First note that F contains a subfield isomorphic to $\mathbb{F}_p$, namely the one generated by 1. Now consider the group F^* of units in F. Since F is finite, let k be the order of F^*. Then for any $x \in F^*$, $x^k = 1$. Thus, $x^k - 1 = 0$ for all $x \in F^*$, proving that all elements of F are algebraic. (Since 0 is obviously algebraic.)

7.4.11

Represent the field $\mathbb{Q}(e^{\frac{2\pi i}{3}})$ as a quotient of of $\mathbb{Q}[x]/(f(x))$. Note that $\omega = e^{\frac{2\pi i}{3}}$ satisfies $\omega^3 = 1$, but $\omega^n \neq 1$ for $0 < n < 3$. Thus ω is called a *primitive third root of unity.*

Solution:

The polynomial $x^3 - 1$ has a single root over $\mathbb{Q}$, specifically 1 is a root. We have the polynomial divison $x^3 - 1 : (x - 1) = x^2 + x + 1$, and this polynomial is irreducible over $\mathbb{Q}$. Also $e^{\frac{2\pi i}{3}}$ is a root of $x^2 + x + 1$, since it is a root of $x^3 - 1$. Since it has degree 2, $x^2 + x + 1$ must therefore be the minimal polynomial of $e^{\frac{2\pi i}{3}}$ So $\mathbb{Q}(e^{\frac{2\pi i}{3}}) \simeq \mathbb{Q}[x]/(x^2 + x + 1)$ (Proposition 7.4.2).

7.4.12

Do the analog of the preceding exercise but with $\mathbb{Q}$ replaced with $\mathbb{F}_2$.

Solution:

Again $x^2 + x + 1$ is a minimal polynomial for a primitive third root of unity. Since $1^2 + 1 + 1 \neq 0$ and $0^2 + 0 + 1 \neq 0$, the polynomial is irreducible. To see that it is a minimal polynomial for a third root of unity, let ω be a root of $x^2 + x + 1$. If a^2 or a is equal to 1, then $a^2 + a + 1$ is equal to either a or a^2. (Remember we work in characteristic 2), contradicting that a is a root of $x^2 + x + 1$. We now compute a^3. Since $a^2 = -a - 1 = a + 1$, we have

$$a^3 = a(a + 1) = a^2 + a = a^2 + a - 0 = a^2 + a - (a^2 + a + 1) = -1 = 1$$

Thus, $x^2 + x + 1$ is a minimal polynomial for ω a primitive root of unity, and we get

$$F_2(\omega) \simeq \mathbb{Q}[x]/(x^2 + x + 1)$$