Exam questions ALGZTH

ScyllaHide

26. Juli 2020

Let $p \in \mathbb{N}$ prime, $K \subseteq E \subseteq F$ fields, $[E\colon K] < \infty$ and $m \in K[x]$ the minimal polynomial of $\alpha \in E$. prove the follwoing claims:

(1A) <u>There exists a field with 4 elements.</u> Add some context, we have $\mathbb{F}_p$ with p prime and field with 4 elements (2^2, with $m = 2$) and $\mathbb{F}_2 \subseteq K$ field ext.

proof. We need $f \in \mathbb{F}_2[x]$ monic, irreducible, degree 2. We find $f = x^2 + x + 1$, it is irreducible bcs $f(0) = 1 \wedge f(1) = 1$, since $\mathbb{F}_2 = \{0, 1\}$! With Theorem 3.13 from lecture we have that

$$\mathbb{F}_2[x]/(x^2 + x + 1)$$

is a field again and thats our field with 4 elements we claimed above. theorem 3.13:

Let K be a field and let $f(x) \in K[x]$ be a nonconstant polynomial. Then the following conditions are equivalent.

a) $f(x)$ is irreducible.

b) $K[x]/(f(x))$ is an integral domain.

c) $K[x]/(f(x))$ is a field. $\square$

(1B) <u>$f(x) = x^6 + 1 \in \mathbb{Q}[x]$ consists of two irreducible factors.</u>

proof. We do polynomial division and find that f is represented by

$$\begin{array}{r|l}
 & x^4 - x^2 + 1 \\
\hline
x^2 + 1 & x^6 \qquad\qquad + 1 \\
 & \underline{-x^6 - x^4} \\
 & -x^4 \\
 & \underline{x^4 + x^2} \\
 & x^2 + 1 \\
 & \underline{-x^2 - 1} \\
 & 0
\end{array}$$

now we need to show that these are both irreducible.

- The polynomial $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. But in your case, $f(x+1) = (x+1)2+1 = x2+2x+2$ is irreducible by EISENSTEIN's criterion (with $p = 2$.)
- here we can substitute with $z = x^2$ and get $z^2 + z - 1 = 0$ use $p - q$-formula

$$x_{1/2} = -p/2 \pm \sqrt{p^4/2 - q}$$

we can see that here the sqrt-term is complex, this holds even if we sub back in.

this will give us the desired result. □

(2A) GAUSS's Lemma: Let $f(x)$ be non-constant. Let $f(x) \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Z}$. Then $f(x)$ is also irreducible over $\mathbb{Q}$.

proof. Assume that $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{Q}[x]$ of smaller degree. Multiplying both sides by the product of all denominators of the coefficients of $g(x)$ and $h(x)$ we can write $nf(x) = g'(x)h'(x)$ where now $g'(x), h'(x) \in \mathbb{Z}[x]$.

We now inductively cancel out prime factors of n: let p be a prime factor of n. We claim that if we write

$$g'(x) = g_0 + g_1 x + \cdots g_r x^r, \qquad h'(x) = h_0 + h_1 x + \cdots h_s x^s$$

then p divides all coefficients g_i or all coefficients h_j. To prove this assume that the assertion is wrong. Then there exist smallest values i and j such that p does neither divide g_i nor h_j. However, since p divides all coefficients of $nf(x) = g'(x)h'(x)$ we know that p divides the coefficient of x^{i+j} in $g'(x)h'(x)$, which is given by

$$g_0 h_{i+j} + g_1 h_{i+j-1} + \cdots + g_i h_j + \cdots g_{i+j} h_0.$$

By our choice of i and j, the prime p divides every term in this expression except $g_i h_j$. This is a contradiction to the fact that the entire sum is divisible by p.

We may therefore assume without loss of generality that p divides all coefficients of $g'(x)$. Hence we can write $g'(x) = pg''(x)$ where $g''(x)$ is again contained in $\mathbb{Z}[x]$. We may now divide the equation $nf(x) = pg''(x)h'(x)$ by p, and still remain within $\mathbb{Z}[x]$. Proceeding in this way we see that we can factorise $f(x)$ over $\mathbb{Z}[x]$. □

proof sketch. □

(2B) EISENSTEIN Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a polynomial with integer coefficients. Assume that there exists a prime $p \in \mathbb{N}$ such that

•

a) $a_0, a_1, \dots a_{n-1}$ are divisible by p.

b) a_n is not divisible by p.

c) a_0 is not divisible by p^2. Then $f(x)$ is irreducible over $\mathbb{Q}$.

proof. Due to GAUSS Lemma it suffices to show that $f(x)$ is irreducible over $\mathbb{Z}$. To prove this, assume that $f(x) = g(x)h(x)$ where

$$g(x) = g_0 + g_1 x + \cdots g_r x^r, \qquad h(x) = h_0 + h_1 x + \cdots h_s x^s$$

are polynomials in $\mathbb{Z}[x]$ of degree smaller than $\deg(f(x))$. Then clearly $r, s \geq 1$ and $r + s = n$. Now $g_0 h_0 = a_0$ and iusing assumptions $a)$ and $c)$ we see that p divides precisely one of g_0 and h_0. Without loss of generality let us assume that p divides g_0 but not h_0. If all coeffients g_i were divisible by p then a_n would be divisible by p, which contradicts assumption $b)$. Hence there exists a smallest index $j < n$ such that g_j is not divisible by p. Observe that

$$a_j = g_0 h_j + g_1 h_{j-1} + \cdots + g_j h_0 \Rightarrow g_j h_0 = -g_0 h_j - g_1 h_{j-1} - \cdots - g_{j-1} h_1 + a_j$$

is divisible by p due to $a)$, so since g_j is not divisble by p, h_0 is divisible by p, which contradicts our previous observation that only one of g_0, h_0 is divisible by p. □

proof sketch. □

(3A) Tower-law: $[F\colon K] = [F\colon E][E\colon K]$. Let $K \subset E \subset F$ be field extensions. If $F|E$ and $E|K$ are finite then $F|K$ is finite and

$$[F : K] = [F : E][E : K].$$

Moreover $[F : K]$ is infinite iff $[F : E]$ or $[E : K]$ is infinite.

proof. Assume first that $F|E$ and $E|K$ are finite. Let $\alpha_1, \dots, \alpha_m$ be a K-basis of E and let $\beta_1, \dots, \beta_n$ be an E-basis of F. Then the elements $\alpha_i \beta_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ form a K-basis of F. Indeed, every element γ of F can be written as a linear combination

$$\gamma = \sum_{j=1}^{n} \lambda_j \beta_j$$

where $\lambda_j \in E$ for every j. Therefore we can write

$$\lambda_j = \sum_{i=1}^{m} \mu_{ij} \alpha_i$$

for uniquely determined elements $\mu_{ij} \in K$, and we obtain

$$\gamma = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{ij} \alpha_i \beta_j.$$

This shows that the vectors $\alpha_i\beta_j$ form a generating set for F as a K-vector space. Now assume that

$$\sum_{j=1}^{n}\sum_{i=1}^{m}\mu_{ij}\alpha_i\beta_j = 0$$

for some coefficients $\mu_{ij} \in K$. Since the β_j form an E-basis of F we conclude

$$\sum_{i=1}^{m}\mu_{ij}\alpha_i = 0$$

for all $j = 1, \ldots, n$. Since the α_i form a K-basis of E it follows that $\mu_{ij} = 0$ for all i, j. This means that the vectors $\alpha_i\beta_j$ are linearly independent.

The same arguments work with minor modifications if $F|E$ or $E|K$ are infinite. In particular, we obtain a K-basis of infinite length for F if one of $[E : F]$ or $[E : K]$ are infinite. □

proof sketch. test □

(3B) $[F\colon K] = p$, then $F|K$ simple. see link ...

(4A) minimal polynomial of $\exp(\mathrm{i}\pi/4) \in \mathbb{C}$ over $\mathbb{Q}$ is $x^4 + 1$.

solution. okay when we take $\exp(\mathrm{i}\pi/4) \in \mathbb{C}$, we find it is a root of $x^4 + 1$, it is irreducible when we take a look at the automorphisms $f(x + 1) = (x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, so use EISENSTEIN for $p = 2$, there u gooooo!

why is this an autmorphism? well we can use the universal property of polynomial rings. □

(4B) $\mathbb{Z}_p$ is splitting field of $x^p - x \in \mathbb{Z}[x]$.

proof. □

(5A) $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \cong \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

proof. – $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$: $\mathbb{Q}$ conjugate of $\sqrt{2}$: $\mathrm{MinPol}(\sqrt{2} \mid \mathbb{Q}) = x^2 - 2$ and $\alpha_1 = -\sqrt{2} \wedge \alpha_2 = \sqrt{2}$
$\mathbb{Q}$ conjugate of $\sqrt{3}$: $\mathrm{MinPol}(\sqrt{2} \mid \mathbb{Q}) = x^2 - 3$ and $\alpha_1 = -\sqrt{3} \wedge \alpha_2 = \sqrt{3}$. then we can construct a

$$c \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

such that

$$c \notin \{\frac{-\sqrt{2} - \sqrt{2}}{+\sqrt{3} + \sqrt{3}} = -\frac{\sqrt{2}}{\sqrt{3}}, \frac{\sqrt{2} - \sqrt{2}}{\ldots} = 0\}$$

so $\gamma = \sqrt{2} + c\sqrt{3} \implies \mathbb{Q}(\sqrt{2}, \sqrt{3}) \overset{(*)}{=} \mathbb{Q}(\gamma)$, so $c = 1!$, where we use the primitive element theorem $(*)$

– $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$: bcs of closure (field property) $(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}(\sqrt{2},\sqrt{3})$.

$\square$

(5B) Is $E = K(\alpha)$, then holds $E \cong K[x]/(m)$.

(6A) some constructible shit ...

(6B) some constructible shit ... :(

(7A) $E|K$ is normal $\iff E$ is splitting field of $f \in K[x]$. prop 5.13

proof. *a)* $\Rightarrow$ *b)* Since $E|K$ is finite we can write $E = K(\alpha_1, \ldots, \alpha_n)$ for some elements $\alpha_1, \ldots, \alpha_n \in E$. If $f_j(x)$ is the minimal polynomial of α_j then $f_j(x)$ splits over E into linear factors by normality. We conclude that $E|K$ is the splitting field of $f(x) = f_1(x)f_2(x)\cdots f_n(x)$.

b) $\Rightarrow$ *a)* Assume that E is the splitting field of $f(x) \in K[x]$. Let $g(x) \in K[x]$ be any irreducible polynomial with a zero in E. We have to show that $g(x)$ splits in $E[x]$. To this end let F be a splitting field of $f(x)g(x)$ such that $E \subset F$ (e.g. view $g(x)$ as an element of $E[x]$ and adjoin the zeros of $g(x)$ in an algebraic closure $\bar{E}$ to E). Moreover let $\beta_1, \beta_2 \in F$ be zeros of $g(x)$. We claim that

$$[E(\beta_1) : E] = [E(\beta_2) : E]. \tag{1}$$

This is proved as follows. Consider the towers of fields

$$K \subset K(\beta_1) \subset E(\beta_1) \subset F$$
$$K \subset K(\beta_2) \subset E(\beta_2) \subset F.$$

For $j = 1, 2$ we have

$$[E(\beta_j) : E][E : K] = [E(\beta_j) : K] = [E(\beta_j) : K(\beta_j)][K(\beta_j) : K]. \tag{2}$$

Since $g(x) \in K[x]$ is irreducible we have a K-isomorphism $K(\beta_1) \cong K(\beta_2)$ according to Corollary **??**, in particular

$$[K(\beta_1) : K] = [K(\beta_2) : K]. \tag{3}$$

Now $E(\beta_j)$ is the splitting field of $f(x)$ over $K(\beta_j)$, and by Theorem **??** we conclude that $E(\beta_1) \cong E(\beta_2)$ and

$$[E(\beta_1) : K(\beta_1)] = [E(\beta_2) : K(\beta_2)]. \tag{4}$$

Combining equations (4), (2) and (3) we obtain equation (1) as desired.

Now if $\beta_1 \in E$ then $E(\beta_1) = E$ and therefore $[E(\beta_1) : E] = 1$. By our above considerations we deduce $[E(\beta_2) : E] = 1$, which in turn means $\beta_2 \in E$. That is, if $g(x)$ has a zero in E then every other zero of $g(x)$ will be contained in E as well. This means that $E|K$ is normal. $\square$

(7B) primitive element theorem. (use FEHM version here!) Let $E|K$ be a finite separable extension ($[K\colon E] < \infty$). Then there exists $\alpha \in E$ such that $E = K(\alpha)$.

proof. It is enuff $E = K(\alpha, \beta)$ with β separable over K to consider. Let $\alpha = \alpha_1, \ldots, \alpha_n$ and $\beta = \beta_1, \ldots, \beta_m$ the K conjugated of α and β. Because K is infinite can we find a $c \in K$ with

$$\textit{content...}$$

todo □

(8A) The galois group of $x^4 + 1 \in \mathbb{Q}[x]$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$

(8B) Lemma 7.15 from lecture notes

list of of important definitions and shit:

- polynomial
- irreducible
- degree of field extension
- minimal polynomial and splitting field
- simple field extension
- n- labllabl
- normal and separable field extension
- galois extension and galois group / might add galois correspondence here.