Algebra II: Homework 9

Due on April 07, 2021

Professor Walton

Gabriel Gress

Last edited April 7, 2021

Collaborated with the Yellow group.

Problem 1

Claim. Suppose that K is a separable field extension of F, and E is an intermediate field so that $F \subset E \subset K$. Prove that:

(i). K is separable over E, and

(ii). E is separable over F.

Proof. (i). Let $\alpha \in K$ be given. Because K is a separable field extension of F, we have that α is the root of a separable polynomial in $F[x]$. But because $F \subset E$, any polynomial $f(x) \in F[x]$ is in $E[x]$, so α is the root of a separable polynomial in $E[x]$, and hence K is separable over E.

(ii). To see that E is separable over F, we let $\alpha \in E$ be given. Of course, because $E \subset K$, $\alpha \in K$, and hence α is the root of a separable polynomial in $F[x]$, giving E separability over F.

□

Problem 2

Claim. Suppose $K[x]$ is a polynomial ring over the field K and F is a subfield of K. If F is a perfect field and $f(x) \in F[x]$ has no repeated irreducible factors in $F[x]$, prove that $f(x)$ has no repeated irreducible factors in $K[x]$.

Proof. By definition, f is separable and has distinct roots in $\overline{F}$. Let $\alpha_i \in \overline{F}$ represent the distinct roots of f. Note that $\alpha_i \in \overline{K}$ as $\overline{F} \subset \overline{K}$.

This tells us that f cannot have a repeated irreducible factor in $K[x]$. If it did, then this repeated irreducible factor must have some α_i as a root, and hence the root would be repeated in $F[x]$, which cannot occur by hypothesis. Thus $f(x)$ has no repeated irreducible factors in $K[x]$. □

Problem 3

Claim. Prove that $d \mid n$ if and only if $x^d - 1 \mid x^n - 1$.

Use this to conclude that if $a > 1$ is an integer then $d \mid n \iff a^d - 1 \mid a^n - 1$, and then conclude that $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \iff d \mid n$.

Proof. Let $d \mid n$ and write $n = qd$ for some q. Then

$$x^{qd} - 1 = (x^d - 1)(x^{qd-d} + x^{qd-2d} + \ldots + x + 1)$$

and hence $x^d - 1$ is a factor, as desired. Now assume the converse, so that $x^d - 1 \mid x^n - 1$. Let $n = qd + r$ for some $r < d$. Then

$$x^{qd+r} - 1 = x^r(x^{qd} - 1) + (x^r - 1) = (x^d - 1)(x^{qd-d} + \ldots + x + 1) + (x^r - 1)$$

Problem 3 continued on next page...

Now observe that because $x^d - 1$ divides the first term, in order for $x^d - 1 \mid x^n - 1$, it must divide the second term as well. But $x^d - 1 \mid x^r - 1$ for $r < d$ only when $r = 0$, and hence $n = qd$ as desired.

This gives us the result for α an integer, as needed. Now observe that

$$p^d - 1 \mid p^n - 1 \iff x^{p^d - 1} - 1 \mid x^{p^n - 1} - 1 \iff x^{p^d} - x \mid x^{p^n} - x$$

This implies that the roots of $x^{p^d} - x$ must all be roots of $x^{p^n} - x$ and hence that $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Because $d \mid n \iff p^d - 1 \mid p^n - 1$, the iff's carry through and thus

$$d \mid n \iff \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}.$$

□

Problem 4

Claim. For any prime p and any nonzero $a \in \mathbb{F}_p$, prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$.

Proof. To see that $x^p - x + a$ is separable over $\mathbb{F}_p$, we will show that every element of $\mathbb{F}_p$ is a root of f. Let α be a root of f. Observe that

$$f(\alpha + 1) = (\alpha + 1)^p - \alpha - 1 + a = \alpha^p + 1 - \alpha - 1 + a = \alpha^p - \alpha + 1 = f(\alpha) = 0.$$

Note that the third equality holds because we are in $\mathbb{F}_p$. This shows that $\alpha + 1$ is a root if α is a root, and thus because there exists a root of f in $\mathbb{F}_p$, it must hold that every element of $\mathbb{F}_p$ is a root.

To show irreducibility, we observe that there are no linear factors. Suppose we have a factor with degree greater than or equal to 2. Because it cannot have a repeated factors, if it has a root, it must have at least one additional root. But because we have $\alpha + 1$ is a root if α is a root, then we know that if α is a root, then there must be a distinct root of the form $\alpha + j$. But we can iterate this until we have p roots, in which case the factor must be $x^p - x + a$ itself; and hence the only factor of degree greater than 2 is the polynomial itself. □

Problem 4 continued on next page. . .

Problem 5

Claim. Let F be the quotient field of the polynomial ring $\mathbb{F}_2[t]$, that is, F consists of fractions $f(t)/g(t)$, for $f(t), g(t) \in \mathbb{F}_2[t]$ with $g(t) \neq 0$, with addition and multiplication performed as one typically adds and multiplies fractions. Consider the polynomial $f(x) = x^2 - t \in F[x]$. Show that:

(i). $f(x)$ is irreducible in $F[x]$

(ii). $f(x)$ is not separable in $F[x]$.

Proof. (i). We want to show that $x^2 - t$ cannot be expressed as $f(t)/g(t)$ for $f, g \in \mathbb{F}_2[t]$. Assume for the sake of contradiction that there is a root $\frac{f}{g}$ in $F[x]$. Then $\frac{f^2}{g^2} = t$. But both f^2, g^2 have even degree, and so their quotient have even degree. But t is of degree one, and so equality cannot hold.

(ii). We want to show that $f(x)$ has a repeated root. Observe that $x^2 - t = (x - \sqrt{t})(x + \sqrt{t})$. We want to show that there exists a field extension in which $-\sqrt{t} = \sqrt{t}$. If $\frac{f}{g} = \sqrt{t}$, then $\frac{f^2}{g^2} = t$. which holds in $\mathbb{F}_2(\sqrt{t})$ as $2 \cdot x = 0$ in $\mathbb{F}_2$, and so we have that $f(x)$ is not separable.

□

Problem 6

Claim. Prove Fermat's Little Theorem: if p is prime and c is an integer, then $c^p \cong c \mod p$.

Proof. Recall that the splitting field of $x^p - x$ is $\mathbb{Z}_p$. Thus $x^p - x$ factors into linear factors in $\mathbb{Z}_p$, and because the degree of the polynomial is p, has p roots in $\mathbb{Z}_p$. Because $x^p - x$ is separable, none of the roots are repeated. Thus because $\mathbb{Z}_p$ has p elements, each element must be a root of $x^p - x$. This is precisely equivalent to $c^p \cong c \mod p$ for $c \in \mathbb{Z}$. □

Problem 6 continued on next page...