HOMEWORK-5

SIDDHANT CHAUDHARY
BMC201953

35. Artin Chapter 15: 3.8.

Solution. Let $\alpha, \beta \in \mathbb{C}$ such that $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers. We show that α, β are also algebraic numbers.

First, we show that the set of algebraic numbers is closed under square roots. So, suppose $\gamma \in \mathbb{C}$ is such that $p(\gamma) = 0$ for some $p(x) \in \mathbb{Q}[x]$. Then, we see that $p(\sqrt{\gamma}^2) = 0$, i.e $\sqrt{\gamma}$ is a root of the polynomial $p(x^2) \in \mathbb{Q}[x]$.

So now, observe that

$$\alpha - \beta = \sqrt{(\alpha+\beta)^2 - 4\alpha\beta}$$

The number inside the square root is algebraic, and hence it follows that $\alpha - \beta$ is also algebraic. So,

$$2\alpha = \alpha + \beta + \alpha - \beta$$

is also algebraic, implying that α is algebraic. Similarly, it can be shown that β is also algebraic, and this completes the proof. ■

36. Artin Chapter 15: 3.9.

Solution. Let $f(x), g(x) \in \mathbb{Q}[x]$ be irreducible polynomials, and let α, β be complex roots of these polynomials. Let $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$. We will show that $f(x)$ is irreducible in $L[x]$ if and only if $g(x)$ is irreducible in $K[x]$. Moreover, we will only show one direction of the proof, as the other direction is completely symmetric. First, we know that

$$K \cong \frac{\mathbb{Q}[x]}{(f(x))} \quad , \quad L \cong \frac{\mathbb{Q}[x]}{(g(x))}$$

Now, suppose $g(x)$ is irreducible in $K[x]$. So, this means that the following are fields:

$$\frac{K[x]}{(g(x))} \cong \frac{\mathbb{Q}[x]/(f(x))}{(\overline{g(x)})} \cong \frac{\mathbb{Q}[x])}{(f(x), g(x))} \cong \frac{\mathbb{Q}[x]/(g(x))}{(\overline{f(x)})} \cong \frac{L[x]}{(f(x))}$$

where above we have used the **Third Isomorphism Theorem**. So, this implies that $f(x)$ is irreducible in $L[x]$. As we said before, the converse is similar to proof, and hence this completes the proof. ■

Date: December 2020.

37. Artin Chapter 15: 6.1.

Solution. Let F be a field of characteristic zero. Let f' be the derivative of f, and let $g \in F[x]$ be an irreducible polynomial that is a divisor of both f and f'. We show that g^2 divides f.

The key fact we will be using is this: since F is a field of characteristic 0, if $h(x) \in F[x]$ is any non-zero polynomial of degree atleast 1, then $h'(x) \neq 0$. The proof of this is immediate.

Since $g(x) \in F[x]$ is irreducible, we see that deg$(g(x)) \geq 1$ and that $g'(x) \neq 0$. If $f = 0$, then there is nothing to prove. So, suppose $f \neq 0$. Then, we can write

$$f(x) = q(x)g(x)$$

for some $q(x) \in F[x]$, $q \neq 0$. This immediately implies that deg$(f(x)) \geq 1$, and hence $f' \neq 0$. Moreover, we have that

$$f'(x) = q'(x)g(x) + q(x)g'(x)$$

Because we are given that $g(x) \mid f'(x)$, we immediately see that $g(x) \mid q(x)g'(x)$ from the above equation. Now, $g(x)$ is an *irreducible* in the UFD $F[x]$, and hence it is prime. Also, $g(x) \nmid g'(x)$, because the degree of $g'(x)$ is strictly less than that of g. So, the primality of $g(x)$ implies that $g(x) \mid q(x)$, and hence we conclude that $g^2 \mid f$ in $F[x]$. This completes the proof. ■

Before solving the next problem, I will mention here a fact about finite fields which we have proven in one of the exercises given in Lecture 8.

Theorem 0.1 (**Subfields of Finite Fields**). *Let p be a prime, and let E be a finite field with $|E| = p^n$. Then,*

$$E \text{ contains a unique subfield } M \text{ with } |M| = p^d \iff d \mid n$$

38. Artin Chapter 15: 7.6. Only list *how many factors* of each degree are there. You need not write the actual factorization.

Solution. In this problem, we will describe the factorisations of the polynomial $x^{16} - x$ over the fields $\mathbb{F}_4$ and $\mathbb{F}_8$.

In $\mathbb{F}_4$. First, consider the following lattice of field extensions (the arrow $F \to K$ will mean that K/F is a field extension).

$$\begin{array}{c} \mathbb{F}_{16} \\ \uparrow \\ \mathbb{F}_4 \\ \uparrow \\ \mathbb{F}_2 \end{array}$$

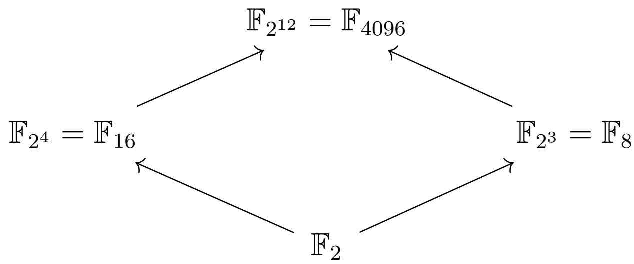
and the existence of this lattice comes from **Theorem** 0.1. Now, we know that the polynomial $x^{16} - x$ completely splits into linear factors in $\mathbb{F}_{16}$, and that each element of $\mathbb{F}_{16}$ is a root of $x^{16} - x$. So, it follows that there are exactly 4 roots of $x^{16} - x$ in $\mathbb{F}_4$, i.e there are exactly 4 linear factors in $\mathbb{F}_4[x]$. Now, suppose $h(x) \in \mathbb{F}_4[x]$ is a monic irreducible factor of $x^{16} - x$ in $\mathbb{F}_4[x]$ with deg$(h(x)) \geq 2$. Again, we see that $h(x)$ has a root in $\mathbb{F}_{16}$, but clearly it doesn't have a root in $\mathbb{F}_4$.

Let $\alpha \in \mathbb{F}_{16}$ be this root. So, if we consider the field extensions $\mathbb{F}_4 \subset \mathbb{F}_4(\alpha) \subset \mathbb{F}_{16}$, then by **Multiplicativity of Degree** in field extensions we see that

$$2 = [\mathbb{F}_{16} : \mathbb{F}_4] = [\mathbb{F}_{16} : \mathbb{F}_4(\alpha)][\mathbb{F}_4(\alpha) : \mathbb{F}_4]$$

i.e $[\mathbb{F}_4(\alpha) : \mathbb{F}_4$ is a factor of 2, which implies that deg$(h(x))$ is a factor of 2, and hence deg$(h(x)) = 2$. So, we have shown that any monic irreducible factor of $x^{16} - x$ is either linear or quadratic. So, it follows that there are exactly 4 linear factors and exactly 6 quadratic irreducible factors of $x^{16} - x$ in $\mathbb{F}_4[x]$.

In $\mathbb{F}_8$. We begin by considering the following lattice of fields, whose existence is guaranteed by **Theorem** 0.1.



Now, we know that the polynomial $x^{16} - x$ completely splits into linear factors in $\mathbb{F}_{16}$, and hence it will complete split into linear factors in $\mathbb{F}_{4096}$. Now, this polynomial has atmost 16 roots, and hence it follows that all the roots belong to the subfield $\mathbb{F}_{16}$. From the above lattice, it follows that $x^{16} - x$ has exactly two roots in $\mathbb{F}_8$, i.e $x^{16} - x$ has exactly two linear factors in $\mathbb{F}_8[x]$.

Now, we know the factorisation of $x^{16} - x$ in $\mathbb{F}_2[x]$: $x^{16} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_2[x]$ of degrees $1, 2$ and 4. There are 2 linear polynomials, 1 monic quadratic irreducible polynomial (which is $x^2 + x + 1$) and three monic irreducible factors of degree 4. Now, the linear polynomials remain irreducible in $\mathbb{F}_8[x]$. Since $\mathbb{F}_8$ contains exactly 2 roots of $x^{16} - x$, it follows that $x^2 + x + 1$ remains irreducible in $\mathbb{F}_8[x]$. Now, we will show that the three monic irreducibles of degree 4 also remain irreducible in $\mathbb{F}_8[x]$, and that will complete our proof.

So let $g(x)$ be any one of irreducibles factors of degree 4 of $x^{16} - x$ in $\mathbb{F}_2[x]$. For the sake of contradiction, suppose $g(x)$ factors into two quadratic factors in $\mathbb{F}_8[x]$ (there can be no linear factors as $\mathbb{F}_8$ contains exactly two roots of $x^{16} - x$). First, let $\beta \in \mathbb{F}_8$ be such that $\mathbb{F}_2(\beta) = \mathbb{F}_8$ (we can let β to be the generator of the cyclic group $\mathbb{F}_8^{\times}$). Since $g(x) \mid x^{16} - x$, $\mathbb{F}_{16}$ contains a root α of $g(x)$. So, we see that $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$. Again, $\alpha \notin \mathbb{F}_8$, but because α satisfies $g(x)$, it satisfies a quadratic irreducible polynomial in $\mathbb{F}_8[x]$, and hence $[\mathbb{F}_8(\alpha) : \mathbb{F}_8] = 2$. But, because $\mathbb{F}_8 = \mathbb{F}_2(\beta)$, by **Multiplicativity of Degree** this implies that

$$[\mathbb{F}_2(\alpha, \beta) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha, \beta) : \mathbb{F}_8][\mathbb{F}_8 : \mathbb{F}_2] = [\mathbb{F}_8(\alpha) : \mathbb{F}_8][\mathbb{F}_8 : \mathbb{F}_2] = 6$$

so that $\mathbb{F}_2(\alpha, \beta) \cong \mathbb{F}_{2^6} = \mathbb{F}_{64}$. But, it is easy to see that $\mathbb{F}_{64}$ *does not* contain $\mathbb{F}_{16} = \mathbb{F}_2(\beta)$ by **Theorem** 0.1. So, this contradicts the fact that $g(x)$ splits into two quadratic factors in $\mathbb{F}_8[x]$, and hence $g(x)$ remains irreducible in $\mathbb{F}_8[x]$. So it follows that the factorisation of $x^{16} - x$ over $\mathbb{F}_8$ is the same as that over $\mathbb{F}_2$. ■

Proposition 0.2. *Let F be a finite field with $|F| = p^n$. Then, the Frobenius map $x \mapsto x^p$ is an automorphism of F.*

Proof. Since F has characteristic p, we already know that the Frobenius map is a homomorphism. So, we only need to show that this map is bijective. We know that $F^\times$ is cyclic; so let α be a generator. So, any non-zero element of F is of the form α^k for some $k \in \mathbb{Z}$, and hence this is mapped to $\alpha^{pk} \neq 0$, showing that the kernel of the map is zero, and hence the map is injective. Since F is a finite set, any injective map from F to itself must be surjective. This completes the proof. ■

39. Artin Chapter 15: 7.10 (Hint: prove it is a p^{th} power).

Solution. Let F be any finite field, and let $f(x)$ be a non-constant polynomial whose derivative is the zero polynomial. Then we show that f cannot be irreducible over F.

Suppose $|F| = p^n$. Because $f(x)$ is a non-constant polynomial, it has a term of degree atleast 1. So, let $a_k x^k$ be a term of $f(x)$, where $a_k \neq 0$ and $k \geq 1$. Because $f' = 0$, we see that $ka_k = 0$, and this implies that $k = 0$ in $\mathbb{F}_p$, i.e $k = pj$ for some $j \in \mathbb{Z}$. So, this implies that $f(x)$ is of the form

$$f(x) = \sum_{i=0}^{m} a_i x^{pi}$$

for $a_i \in F$. By **Proposition** 0.2, we know that $x \mapsto x^p$ is an automorphism of F. So, for each $0 \leq i \leq m$, there is some $b_i \in F$ such that $a_i = b_i^p$, and hence

$$f(x) = \sum_{i=0}^{m} (b_i x^i)^p$$

Now, the ring $F[x]$ has characteristic p, and hence the Frobenius map on this ring is a homomorphism. So, we see that

$$f(x) = g(x)^p$$

where

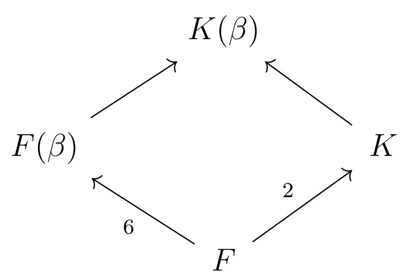
$$g(x) = \sum_{i=0}^{m} b_i x^i$$

Because f is a non-constant polynomial, it follows that g is also a non-constant polynomial, and hence it follows that f is not irreducible over F. ■

40. Artin Chapter 15: M.3.

Solution. Let $f(x) \in F[x]$ be an irreducible polynomial of degree 6 for some field F, and let K/F be a quadratic extension of F. Let K_1 be an extension of F with $F \subset K \subset K_1$ such that K_1 contains all roots of f.

Now, let $\beta \in K_1$ be a root of f. So, we see that $[F(\beta) : F] = 6$. Now, consider the following lattice of fields.



So, we see that $[K(\beta) : F] \leq 6 \cdot 2 = 12$. The above diagram also implies that $[F(\beta) : F]$ divides $[K(\beta) : F]$, and hence $6 \mid [K(\beta) : F]$, implying that $[K(\beta) : F] \in \{6, 12\}$. Now, because

$$[K(\beta) : F] = [K(\beta) : K][K : F] = 2[K(\beta) : K]$$

we see that $[K(\beta) : K] \in \{3, 6\}$. So, if $[K(\beta) : K] = 6$, then $f(x)$ does not split into any factors in $K[x]$, i.e it stays irreducible in $K[x]$.

If $[K(\beta) : K] = 3$, then $f(x)$ has an irreducible factor of degree 3 in $K[x]$. So, suppose $f(x) = g(x)h(x)$ in $K[x]$, where $g(x)$ is the irreducible factor of $f(x)$. Clearly, $h(x) \in K[x]$ has degree 3. We claim that $h(x)$ must be irreducible as well. For the sake of contradiction, suppose $h(x)$ is not irreducible over $K[x]$; so, it has a root γ in K (because it has degree 3). Clearly, $\gamma \notin F$, because f is irreducible in $F[x]$. So, it follows that $\gamma \in K - F$. Because $[K : F] = 2 < \infty$, γ is algebraic over F. For the tower of fields $F \subset F(\gamma) \subset K$, we see that $2 = [K : F(\gamma)][F(\gamma) : F]$, and hence $[F(\gamma) : F] = 2$ since $\gamma \notin F$. So, this implies that the minimal polynomial of γ over F has degree 2, and it divides f. But, this contradicts the fact that f is irreducible over F. So, it follows that $h(x) \in K[x]$ must be irreducible.

So, the only possible degrees of the irreducible factors of f in $K[x]$ are 3 and 6. ■