Math 1540: HW1

February 24, 2023

Book Problems:

72. (i) Since α and β are algebraic over F there exist monic irreducible polynomials p_1 and p_2 of finite degree with roots α and β respectively. Therefore, we can say that $[F(\alpha) : F] = \deg(p_1)$ and $[F(\alpha, \beta) : F(\alpha)] = \deg(p_2)$ and using the degree formula we can see that $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = \deg(p_1) \cdot \deg(p_2)$. Moreover, this is a finite degree extension. Finally, we can use the fact if E / F is a finite extension, then it is an algebraic extension to show that every element of $F(\alpha, \beta)$ (ex. $\alpha + \beta$, $\alpha\beta$, α^{-1}) is algebraic over F

    (ii) K contains F: $\forall x \in F$ x is algebraic over F so $\forall x \in F$ $x \in K$

    K is a subfield of E: For all x in K but not F we know that from the prior result that x^{-1}, $x + y$ where $y \in F$, xy where $y \in F$, etc. are all algebraic. This shows that K is closed and contains additive/multiplicative inverses. Moreover, K has additive and multiplicative identities from F and gets associativity, commutativity, distributivity laws from E. Therefore, K is a field. By definition $K \subseteq E$. Therefore, K is a subfield of E.

    (iii) $\mathbb{A}/\mathbb{Q}$ is not finite since it must contain all roots of polynomials of the form $x^2 - p$ where p is prime, which would require $\mathbb{Q}$ have a nonfinite extension with $\mathbb{Q}(\sqrt{2}, \sqrt{3} \ldots \sqrt{p} \ldots)$, and we know that there are an infinite number of primes.

76. Suppose that there exists some $a \in F$ s.t. a does not have a pth root in F. Let $b^p = a$ in an extension of F. Therefore, in $F[x]$, there exists $x^p - a = x^p - b^p = (x - b)^p$. If $x^p - a$ is not irreducible over F, then $(x - b)^i$ where $1 \leq i \leq p - 1$ must be a factor in $F[x]$ and all its coefficients must be in F. $(x - b)^i = x^i - ibx^{i-1} \ldots$, so $-ib \in F$ so $b^p = a \in F$, but we assumed a does not have a pth root in F — contradiction. Therefore, $x^p - a$ is irreducible. From here we see that irreducible polynomials must be inseparable, because if they weren't, they could be reduced by using arithmetic in characteristic p

77. Let F be a finite field of characteristic p, φ be the map from F to itself where $\forall x \in F$ $\varphi(x) = x^p$

    From this map it is evident:

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$$
$$\varphi(x + y) = (x + y)^p = x^p + y^p$$

    Moreover, φ is injective since $x^p \neq 0$; therefore it is surjective (F is finite) and $F^p = F$ — F is perfect

Given Problems:

1. Let the field of fractions be written as $Frac(F[x]) = \{f(x)/g(x) \in E \mid f, g \in F[x] \text{ and } g(x) \neq 0\}$. Let φ be a map between $F[x]$ and $Frac(F[x])$ where φ sends $f(x) \in F[x]$ to $f(x)/1$. This map is well defined since $f(x) = g(x) \Rightarrow \varphi(f(x)) = f(x)/1 = g(x)/1 = \varphi(g(x))$. And injective since only 0 is sent to $\varphi(0) = 0/1$. Moreover, since $F(x)$ is a field if $x \in E/F$ we can construct the inverse map σ from $Frac(F[x])$ to $F[x]$ where σ sends $f(x)/g(x)$ to $f(x)g^{-1}(x) \in F[x]$. This map is well defined since $f_1(x)/f_2(x) = g_1(x)/g_2(x) \Rightarrow \sigma(f_1(x)/f_2(x)) = f_1(x)f_2^{-1}(x) = g_1(x)g_2^{-1}(x) = \varphi(g_1(x)/g_2(x)) \Leftrightarrow f_1(x)g_2(x) = g_1(x)f_2(x)$. Moreover, it is surjective since $\sigma(f(x)/1) = f(x)$ for all $f(x) \in F[x]$. Therefore, there is an isomorphism between $Frac(F[x])$ and $F(x)$

2. Although I could show that $f(x)$ has no linear factors since $f(0) \neq 0, f(1) \neq 0$ and no irreducible quadratic factor (of which there is one $x^2 + x + 1$ and $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f(x)$) (what I've written so far is sufficient for irreducibility), we can use Rabin's test:

   Rabin's test of Irreducibility:

   Let $f(x)$ be a polynomial of degree n over $\mathbb{F}_p$. Then f is irreducible over $\mathbb{F}_p$ if and only if $f(x)$ divides $x^{p^n} - x$, and $\gcd\left(f(x), x^{p^{n/q}} - x\right) = 1$ for each prime divisor q of n.

   Here it is sufficient to show that $\gcd(x^4 + x + 1, x^{2^4} - x)$ is a multiple of $x^4 + x + 1$ and that $\gcd(x^4 + x + 1, x^{2^2} - x) = 1$

   I've computed both calculations in Mathmatica:

   $$\text{PolynomialExtendedGCD}[x^4 + x + 1, x^{2^4} - x, x, Modulus- > 2][[1]] = x^4 + x + 1$$
   $$\text{PolynomialExtendedGCD}[x^4 + x + 1, x^{2^{4/2}} - x, x, Modulus- > 2][[1]] = 1$$

   Therefore, both criteria are satisfied, so $x^4 + x + 1$ is irreducible in $\mathbb{Z}_2$. Therefore, E, the splitting field of $x^4 + x + 1$, has the same degree of $x^4 + x + 1$, 4.

3. We find that $1/\sqrt{2 + \sqrt{3}} = \sqrt{2 - \sqrt{3}}$ from the following:

   $$\frac{1}{\sqrt{2-\sqrt{3}}}$$
   $$\frac{1}{\sqrt{2-\sqrt{3}}}\frac{\sqrt{2+\sqrt{3}}}{\sqrt{2+\sqrt{3}}}$$
   $$\frac{\sqrt{2+\sqrt{3}}}{\sqrt{2-\sqrt{3}}\sqrt{2+\sqrt{3}}}$$
   $$\frac{\sqrt{2+\sqrt{3}}}{\sqrt{(2-\sqrt{3})(2+\sqrt{3})}}$$
   $$\frac{\sqrt{2+\sqrt{3}}}{\sqrt{1}}$$
   $$\sqrt{2+\sqrt{3}}$$

Therefore, $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ will contain $\sqrt{2-\sqrt{3}}$ as the multiplicative inverse of $\sqrt{2+\sqrt{3}}$ and thus will contain $\mathbb{Q}(\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}})$, and it is evident that $\mathbb{Q}(\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}})$ contians $\mathbb{Q}(\sqrt{2+\sqrt{3}})$, so $\mathbb{Q}(\sqrt{2+\sqrt{3}}) = \mathbb{Q}(\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}})$.

Therefore, the extension $\mathbb{Q}(\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}})$ is simple since it can be written as $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ with generating element $\sqrt{2+\sqrt{3}}$

To find the minimal polynomial of $\sqrt{2+\sqrt{3}}$ let's set $x = \sqrt{2+\sqrt{3}}$:

$$\begin{aligned}
\sqrt{2+\sqrt{3}} &= x \\
2+\sqrt{3} &= x^2 \\
\sqrt{3} &= x^2 - 2 \\
3 &= (x^2-2)^2 \\
0 &= (x^2-2)^2 - 3 \\
0 &= x^4 - 4x^2 + 1
\end{aligned}$$

Since the degree of the extension is equal to the degree of the minimal polynomial, the degree of the extension is 4.