172 — 5

RJ Acuña

(862079740)

1. Suppose that F is a finite field with q elements. Let $E \supset F$ be a field extension and suppose $\alpha \in E$ is algebraic over F with degree n. Show that as a set, $F(\alpha)$ has q^n elements.

   slu.

   Since the degree of α over F is n, then $F(\alpha)$ is an $n-$dimensional vector space over F with basis $\mathrm{A} = \{\alpha^k\}_{k=0}^{n-1}$.

   Let, $a_k \in F$, $r \in F(\alpha)$, then $r = \sum_{k=0}^{n-1} a_k\alpha^k$.

   If $n = 1$, then $F(\alpha) = F$, so $|F(\alpha)| = |F| = q$.

   If $n = 2$, then $r = a_0 + a_1\alpha$. There are q possible choices for, a_0 and a_1 respectively. So, there are q^2 possible ways to express r as a linear combination of 1 and α. So, $|F(\alpha)| = q^2$.

   So in general we can think of an element of $F(\alpha)$ as consisting of n-slots $1, \alpha, \dots, \alpha^{n-1}$, and q possible entries a_k. Thus there are at least q^n possible ways to determine an element r of $F(\alpha)$. Since, A is a basis for $F(\alpha)$, r is uniquely determined, so there are at most q^n possible ways to determine r.

   So, $|F(\alpha)| = q^n$ ■

2. Let F be the field $\mathbb{Z}/2\mathbb{Z}$. Find an irreducible polynomial in $F[x]$ of degree 3. Use this to construct a field extension of F that contains 8 elements.

   slu.

   Let $f(x) \in (\mathbb{Z}/2\mathbb{Z})[x]$ be of degree 3. Then,

   $$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0,\ a_i \in \mathbb{Z}/2\mathbb{Z}$$

   There are 2^4 possibilities for $f(x)$, since $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

   If $f(x)$ is reducible, then $f(x) = g(x)r(x)$.

   Since, deg f = deg g + deg r, WLOG assume deg $g = 2$.

   Then the only two possibilities for r are $r(x) = x$ or $r(x) = x + 1$. So if f is reducible,

   $$f(x) = xg(x) \text{ or } f(x) = (x - 1)g(x)$$

   So $f(0) = 0$ or $f(1) = 0$ respectively. If neither $f(0)$ nor $f(1)$ are 0, then $r(x)$ is not a factor of f, thus f is irreducible.

   $$f(0) = a_0 \text{ and } f(1) = \sum_{i=0}^{3} a_i$$

   So, $a_0 \neq 0 \implies a_0 = 1 \implies \sum_{i=0}^{3} a_i = 1 + \sum_{i=1}^{3} a_i$. Since deg $f = 3 \implies a_3 \neq 0 \implies a_3 = 1$. Therefore, $\sum_{i=0}^{3} a_i = 1 + \sum_{i=1}^{2} a_i + 1 = \sum_{i=1}^{2} a_i \neq 0 \implies a_1 = 0$ and $a_2 = 1$ or $a_1 = 1$ and $a_2 = 0$.

   Thus $h(x) = x^3 + x^2 + 1$ and $k(x) = x^3 + x + 1$ are irreducible.

   Since k is irreducible, $\langle k(x)\rangle$ is maximal, thus $E = (\mathbb{Z}/2\mathbb{Z})[x]/\langle k(x)\rangle$ is a field.

   Let $(\mathbb{Z}/2\mathbb{Z})(\alpha)$ be a field extension of $(\mathbb{Z}/2\mathbb{Z})$ such that $k(\alpha) = 0$. Since the degree of α over $(\mathbb{Z}/2\mathbb{Z})$ is equal to the degree of the irreducible polynomial that vanishes at α, the degree of α over $(\mathbb{Z}/2\mathbb{Z})$ is 3. So, by the previous problem it has $2^3 = 8$ elements ◊

3. Find a basis for the field $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ as a vector space over $\mathbb{Q}$.

slu.

$$\begin{aligned}
\alpha = \sqrt{2}+\sqrt{5} &\implies (\alpha-\sqrt{2})^2 = 5 \\
&\implies (\alpha-\sqrt{2})^2 - 5 = 0 \\
&\implies \alpha^2 - 2\alpha\sqrt{2} + 2 - 5 = 0 \\
&\implies \alpha^2 - 3 = 2\alpha\sqrt{2} \\
&\implies (\alpha^2-3)^2 = (2\alpha\sqrt{2})^2 \\
&\implies \alpha^4 - 6\alpha^2 + 9 = 8\alpha^2 \\
&\implies \alpha^4 - 14\alpha^2 + 9 = 0
\end{aligned}$$

Thus $f(x) = x^4 - 14x^2 + 9 \implies f(\sqrt{2}+\sqrt{5}) = 0$

By the quadratic formula, $f(x) = 0$

$$\implies x^2 = \frac{14 \pm \sqrt{196-36}}{2} = \frac{14 \pm \sqrt{160}}{2} = \frac{14 \pm 4\sqrt{10}}{2} = 7 \pm 2\sqrt{10}$$

$$\implies x = \pm\sqrt{7 \pm 2\sqrt{10}}$$

So, f doesn't factor over $\mathbb{Q}$, thus f is irreducible.

Therefore $\{1, \sqrt{2}+\sqrt{5}, (\sqrt{2}+\sqrt{5})^2, (\sqrt{2}+\sqrt{5})^3\}$ is a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ ■

4. Let $E \supset F$ be a field extension and let $\alpha \in E$ be algebraic over F with odd degree. Show that $F(\alpha) = F(\alpha^2)$. Conversely, find an $\alpha \in \mathbb{R}$ which is algebraic over $\mathbb{Q}$ with even degree such that $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\alpha^2)$.

slu.

Since $f(x) = x^2 - \alpha^2 \in F(\alpha^2)[x] \implies f(\alpha) = 0 \implies [F(\alpha) : F(\alpha^2)] = 2$. It follows that,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2[F(\alpha^2) : F]$$

That contradicts that $[F(\alpha) : F]$ is odd.

$\alpha = \sqrt{3} \implies \alpha^2 - 3 = 0 \implies$ deg $\alpha = 2$, and $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(3) = \mathbb{Q}$, since $3 \in \mathbb{Q}$ ■