MATH 7211 Homework 2

Andrea Bourque

May 9, 2023

1 Problem 13.2.7

Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

Proof. If a field contains $\sqrt{2}$ and $\sqrt{3}$, then it must contain $\sqrt{2}+\sqrt{3}$. Thus $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. On the other hand, $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$, so

$$\sqrt{2} = \frac{1}{2}\left((\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})\right),$$
$$\sqrt{3} = \frac{1}{2}\left(11(\sqrt{2}+\sqrt{3}) - (\sqrt{2}+\sqrt{3})^3\right).$$

The right-hand sides in both equations are clearly well-defined expressions in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, so $\sqrt{2}$ and $\sqrt{3}$ are elements of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Thus $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Now, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$. Since $\sqrt{2}$ is a root of $x^2-2 \in \mathbb{Q}[x]$, and $\sqrt{2} \notin \mathbb{Q}$, we have $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. Since $\sqrt{3}$ is a root of $x^2-3 \in \mathbb{Q}(\sqrt{2})[x]$, we have $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] \leq 2$. We must show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Elements in $\mathbb{Q}(\sqrt{2})$ can be written uniquely in the form $a+b\sqrt{2}$ for $a,b \in \mathbb{Q}$. Thus, suppose $\sqrt{3} = a+b\sqrt{2}$ for $a,b \in \mathbb{Q}$. Then $3 = a^2+2b^2+2ab\sqrt{2}$. If $ab \neq 0$, this means $\sqrt{2} = (3-a^2-2b^2)/(2ab) \in \mathbb{Q}$, a contradiction. Thus $a=0$ or $b=0$. If $b=0$, then $\sqrt{3} = a \in \mathbb{Q}$, a contradiction. If $a=0$, then $\sqrt{3/2} \in \mathbb{Q}$, which can be shown to be a contradiction in a few ways:

First, $\sqrt{3/2}$ is a root of $2x^2-3$, which has no rational roots by the rational roots theorem (the theorem says the possible roots are $\pm 3, \pm 3/2, \pm 1, \pm 1/2$, and these can be checked to not be roots). Another way to show $\sqrt{(3/2)} \notin \mathbb{Q}$ is analogous to the classic proof that shows $\sqrt{p} \notin \mathbb{Q}$ for primes p. In particular, if $\sqrt{3/2} = a/b$, where a,b are coprime integers, then $3b^2 = 2a^2$. But an integer of the form $3b^2$ has an odd exponent of 3 in its prime factorization, whereas $2a^2$ has an even exponent of 3. Thus $\sqrt{3/2} \notin \mathbb{Q}$.

We have finally shown that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, so $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$ as desired.

Note that $(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$, so $f(x) = (x^2-5)^2 - 24 = x^4 - 10x^2 + 1$ is an element of $\mathbb{Q}[x]$ with $f(\sqrt{2}+\sqrt{3}) = 0$. Since $f(x)$ is monic and has degree 4, which is the same as the degree of the extension $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$, it must be irreducible. $\square$

2 Problem 13.2.11

(a) Let $\sqrt{3+4i}$ denote the square root of $3+4i$ that lies in the first quadrant and let $\sqrt{3-4i}$ denote the square root of $3-4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}):\mathbb{Q}]=1$.

Proof. Write $3+4i = re^{i\theta}$, where $r \geq 0$ and $0 \leq \theta \leq \frac{\pi}{2}$. We have $r = \sqrt{3^2+4^2} = 5$ and $\theta = \arctan(\frac{4}{3})$. Then $\sqrt{3+4i} = \sqrt{r}e^{i\theta/2}$, since $\theta/2$ lies in the first quadrant. Since $3-4i$ is the conjugate of $3+4i$, we have $3-4i = re^{-i\theta}$, and thus $\sqrt{3-4i} = re^{-i\theta/2}$, since $-\theta/2$ lies in the fourth quadrant. Then

$$\begin{aligned}\sqrt{3+4i}+\sqrt{3-4i} &= \sqrt{5}\left(e^{i\theta/2}+e^{-i\theta/2}\right)\\ &= 2\sqrt{5}\cos\left(\frac{\theta}{2}\right).\end{aligned}$$

Recall $\cos(\theta) = 2\cos^2(\theta/2)-1$. We have $\cos(\theta) = 3/5$ and $\cos(\theta/2) \geq 0$, so $\cos(\theta/2) = 2/\sqrt{5}$. Thus $\sqrt{3+4i}+\sqrt{3-4i} = 4 \in \mathbb{Q}$, so $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}):\mathbb{Q}] = 1$. $\square$

(b) Determine $[\mathbb{Q}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}):\mathbb{Q}]$.

Proof. Note that $1+\sqrt{-3} = 2e^{i\pi/3}$, so $\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}} = 2\sqrt{2}\cos(\pi/6) = \sqrt{6}$. Since $\sqrt{6} \notin \mathbb{Q}$ is a root of $x^2-6 \in \mathbb{Q}[x]$, we have $[\mathbb{Q}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}):\mathbb{Q}] = 2$. $\square$

3 Problem 13.2.12

Suppose $[K : F] = p$ is prime. Show that if field E satisfies $F \subseteq E \subseteq K$, then $E = K$ or $E = F$.

Proof. Since $p = [K : E][E : F]$ is prime, we have that $[K : E] = 1, [E : F] = p$ or $[K : E] = p, [E : F] = 1$. If a field extension has degree 1, then the fields are the same. Thus we have that $E = K$ or $E = F$ as desired. $\square$

4 Problem 13.2.14

Prove that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

Proof. Since $\alpha^2 \in F(\alpha)$, we have $F \subseteq F(\alpha^2) \subseteq F(\alpha)$. Since $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd, $[F(\alpha) : F(\alpha^2)]$ is odd as well. Since α is a root of the polynomial $x^2 - \alpha^2 \in F(\alpha^2)[x]$, we have $[F(\alpha) : F(\alpha^2)] \leq 2$. The only odd positive integer which is less than or equal to 2 is 1, so $[F(\alpha) : F(\alpha^2)] = 1$. Thus $F(\alpha) = F(\alpha^2)$ as desired. □

5 Problem 13.2.16

Let K/F be algebraic, and let R be a ring such that $F \subseteq R \subseteq K$. Show that R is a subfield of K.

Proof. Let $r \in R$ be nonzero. Since $r \in K$, the inverse r^{-1} exists in K. Since K/F is algebraic, r is the root of a non-constant monic irreducible polynomial $f(x) = x^n + ... + a_0 \in F[x]$. Note that $a_0 \neq 0$; otherwise, $f(x) = xg(x)$ would not be irreducible (note that $g(x)$ could not be constant in this case, since $r \neq 0$). Since a_0 is a nonzero element of F, it has an inverse a_0^{-1} in F. Since $F \subseteq R$, we have $a_0^{-1} \in R$ also. Now, as an equation in K, we have

$$-a_0^{-1}(r^{n-1} + ... + a_1) = r^{-1}.$$

The left hand side is a well-defined expression in R, so $r^{-1} \in R$ as desired. □