Graded

1. (13.3.4) The construction of the regular 7-gon amounts to the constructibility of $\cos(2\pi/7)$. We shall see later (Section 14.5 and Exercise 2 of Section 14.7) that $\alpha = 2\cos(2\pi/7)$ satisfies the equation $x^3 + x^2 - 2x - 1 = 0$. Use this to prove that the regular 7-gon is not constructible by straightedge and compass.

   Proof. It suffices to show that the degree of $\alpha = 2\cos(2\pi/7)$ (note $\mathbb{Q}(\alpha) = \mathbb{Q}(\cos(2\pi/7)))$ over $\mathbb{Q}$ is not a power of 2, since if β is a constructible real number, then $[\mathbb{Q}(\beta)\colon \mathbb{Q}]$ is of degree 2^k for some $k \geq 0$.

   The degree of α over $\mathbb{Q}$ is the degree of the minimal polynomial $m_\alpha(x) \in \mathbb{Q}[x]$. It is known that $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. We show that $m_\alpha(x) = x^3 + x^2 - 2x - 1$ by checking that $x^3 + x^2 - 2x - 1$ is monic (it is) and irreducible over $\mathbb{Q}$. We show that this polynomial has no rational roots. The only possible rational roots are ± 1, neither of which satisfy the equation $x^3 + x^2 - 2x - 1 = 0$. Hence the polynomial is irreducible over $\mathbb{Q}$ and so $m_\alpha(x) = x^3 + x^2 - 2x - 1$.

   It follows that $[\mathbb{Q}(\beta)\colon \mathbb{Q}] = \deg(m_\alpha(x)) = 3$, which is not a power of 2 and hence cannot be constructible, meaning the regular 7-gon is not constructible by straightedge and compass. □

2. (13.4.4) Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

   The splitting field over $\mathbb{Q}$ for $x^6 - 4$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ and its degree over $\mathbb{Q}$ is 6.

   Proof. Let $f(x) = x^6 - 4$. Factor (over $\mathbb{C}$ to identify roots) the difference of squares $(x^3)^2 - 2^2$ into $(x^3 - 2)(x^3 + 2)$ and by using the known factorization for sums and differences of cubes we can factor this product further into $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2}) \cdot (x + \sqrt[3]{2})(x^2 - \sqrt[3]{2}x + \sqrt[3]{2^2})$. Using the quadratic formula, we can factor further. We find that the roots of $f(x)$ are

   $$\pm\sqrt[3]{2}, \pm\sqrt[3]{2}\left(\frac{1+\sqrt{-3}}{2}\right), \text{ and } \pm\sqrt[3]{2}\left(\frac{1-\sqrt{-3}}{2}\right).$$

   We show that by adjoining these six roots to $\mathbb{Q}$ we obtain the desired splitting field K of $f(x)$.

   The field K contains 1, $\sqrt[3]{2}$, $\sqrt[3]{2^2}$, the quotient of the positive first two roots above given by $\frac{1+\sqrt{-3}}{2}$ hence also $\sqrt{-3}$, and as a result also contains $\sqrt{-3}\sqrt[3]{2}$ and $\sqrt{-3}\sqrt[3]{2^2}$. Thus K contains the $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ given by $\left\{(\sqrt{-3})^i(\sqrt[3]{2})^j \mid 0 \leq i \leq 1, 0 \leq j \leq 2\right\}$, which implies that $K \supseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. But $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ contains all six roots above, so $K \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Hence $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is the splitting field for $f(x)$.

   To see that the degree of K over $\mathbb{Q}$ is 6, observe that the $\mathbb{Q}$-basis given earlier has exactly 6 elements, or see that because $\sqrt{-3}$ satisfies the equation $x^2 - 3 = 0$ the degree of K over $\mathbb{Q}(\sqrt[3]{2})$ (a cubic extension of $\mathbb{Q}$) is at most 2. But the degree must be 2 since $\sqrt{-3}$ is complex and could not be in $\mathbb{Q}(\sqrt[3]{2})$. Hence $[K\colon \mathbb{Q}] = 6$ as desired. □

Additional Problems

1. (13.2.1) Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.

Proof. Since $\mathbb{F}$ is characteristic p, the unit $1_{\mathbb{F}}$ generates the prime subfield $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{F}$ is an extension of $\mathbb{Z}/p\mathbb{Z}$, we know that there is a *finite* $\mathbb{Z}/p\mathbb{Z}$-basis for $\mathbb{F}$, where this basis is finite because $\mathbb{F}$ is a finite field.

There exist elements $a_1, \dots, a_n \in \mathbb{F}$ for some $n \geq 1$ such that every element in $\mathbb{F}$ is uniquely written as a $\mathbb{Z}/p\mathbb{Z}$-linear combination of $a_1, \dots, a_n$. Counting all the possible ways this combination could go (there are p choices of each of the n coefficients), it follows that $|\mathbb{F}| = p^n$. □

2. (13.2.4) Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

   We have that the degree of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$ is 2 and 3 respectively.

   Proof. The degree of an algebraic element α over a field F is the degree of the minimal polynomial $m_\alpha(x) \in F[x]$.

   The minimal polynomial of $2 + \sqrt{3}$ is $(x-2)^2 - 3 = x^2 - 4x + 1$. It is monic, and irreducible since any potential rational roots would be ± 1, which do not satisfy the equation $x^2 - 4x + 1 = 0$, whereas $2 + \sqrt{3}$ does. Hence the degree of $2 + \sqrt{3}$ over $\mathbb{Q}$ is 2.

   The minimal polynomial of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is $(x-1)^3 - 6x = x^3 - 3x^2 - 3x - 1$. It is monic, and irreducible since any potential rational roots would be ± 1, which do not satisfy the equation $x^3 - 3x^2 - 3x - 1 = 0$, whereas $1 + \sqrt[3]{2} + \sqrt[3]{4}$ does. Hence the degree of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$ is 3. □

3. (13.2.7) Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.]. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

   Proof. Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The inclusion $K \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is clear since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The reverse inclusion is obtained if we can show that every element in a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ may be formed by taking sums/differences/products/quotients of elements of K. Note that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is one $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   Indeed, $1 \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Then see that $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ so that $\sqrt{6} \in K$. Similarly, we have that $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3} \in K$ so that $\sqrt{6}(11\sqrt{2} + 9\sqrt{3}) = 27\sqrt{2} + 22\sqrt{3} \in K$. Then $9(27\sqrt{2} + 22\sqrt{3}) - 22(11\sqrt{2} + 9\sqrt{3}) = \sqrt{2} \in K$. This also means that $\frac{1}{9}(11\sqrt{2} + 9\sqrt{3} - 11\sqrt{2}) = \sqrt{3} \in K$. Since a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is contained in K, the reverse containment $K \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is obtained and so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as desired.

   Observe that $\mathbb{Q}(\sqrt{2})$ is a quadratic extension of $\mathbb{Q}$ which is a subfield of K. It suffices to see that K is a quadratic extension of $\mathbb{Q}(\sqrt{2})$ by adjoining $\sqrt{3}$. The minimal polynomial for $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})[x]$ is $x^2 - 3$, which is monic, and is irreducible since neither $\sqrt{3}, -\sqrt{3}$ lie in $\mathbb{Q}(\sqrt{2})$. It follows that $[K \colon \mathbb{Q}] = 4$.

   With $(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}$, it is easy to find a candidate for an irreducible (and monic) polynomial satisfied by $\sqrt{2} + \sqrt{3}$ since $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$. Consider $f(x) = x^4 - 10x^2 + 1$, which is satisfied by $\sqrt{2} + \sqrt{3}$. It is irreducible over $\mathbb{Q}$: potential rational roots come in the form ± 1, and neither of them are roots, so there is no factorization of $f(x)$ into a linear factor with a cubic polynomial over $\mathbb{Q}$. We must rule out the possibility of $f(x)$ factoring into the product of two quadratics. Factor $f(x)$ over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ by first taking factoring out the two known linear factors (as $\pm(\sqrt{2}+\sqrt{3})$ are roots) to obtain $f(x) = (x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}+\sqrt{3}))(x^2+2\sqrt{6}-5)$. Using the fact that $(\sqrt{2}-\sqrt{3})^2 = -2\sqrt{6}+5$, we can further factor $f(x)$ into $(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x+(\sqrt{2}-\sqrt{3}))$. By exhausting all possible ways to combine factors to write $f(x)$ as a product of quadratic factors (there are 4 choose 2 ways to do this) we find that it is not possible to write $f(x)$ as the product of two quadratic polynomials with rational coefficients. Thus x^4-10x^2+1 is an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$. □

4. (13.2.12) Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

   Proof. With K as an extension of E an extension of F, we have that $p = [K\colon F] = [K\colon E][E\colon F]$. Since p is prime, then one of $[K\colon E]$ and $[E\colon F]$ is 1 and the other is p. If $[K\colon E]$ is 1, then $E = K$ (linear extensions of fields are the same field). Similarly, if $[E\colon F]$ is 1, then $E = F$. □

Feedback

1. (13.2.7) There must be a better/more clever way to show that the polynomial x^4-10x^2+1 is irreducible over $\mathbb{Q}$.

2. Things I think are going okay? So far the topics seem to make sense to me but I guess sometimes I feel a bit uneasy when I have to show that a particular field extension is of a certain degree because there seems to be a handful of ways of doing that and I am not sure which one is the most clear. Perhaps it will just take some practice/time to see if there's a nice strategy.

   I was also thinking about the Algebra seminar a little bit because Recep (one of the participants in the Algebra seminar) came up to me after the preliminary meeting last week and asked me about the REU I had just come out of, and I explained to him in broad strokes what I had done and he suggested I could try giving a talk on the stuff I learned over the summer. Since you're the one organizing the seminar I figure it is worth asking you if the following is something that is okay for the audience of the Algebra seminar:

   I went to Georgia Tech over the summer to study under Dr. Ashley Wheeler a particular family of toric varieties: Let $X = (x_{ij})$ be an $n \times n$ matrix of indeterminates and consider the ideal $I_n = \langle x_{ii}x_{jj} - x_{ij}x_{ji} \mid 1 \leq i < j \leq n\rangle$ generated by all the principal 2-minors of X. It turns out that because this ideal is generated by binomials and it is prime (not obvious, this part was proven in a paper of Dr. Wheeler's), it follows that $\mathbf{V}(I_n)$ (in affine or projective spaces) is a toric variety for each n. This allows us to find and study a family of associated polyhedral objects (this part is why this project was possible for someone of my limited background) to determine certain properties about our toric varieties in both the affine and projective setting. We found that our affine toric varieties were normal but not smooth, but that our projective varieties were normal, separated, compact in both the classical and Zariski topologies, not smooth for $n > 2$, and not orbifolds for $n > 2$ (the definition is way beyond me).

We looked at some of the theory behind toric varieties to help get the project going, but a lot of the actual algebra was blackboxed so my understanding of the most basic theory isn't amazing. There is also a case to be made that this sort of thing is better given as a talk for undergrads given my own understanding of the project or in the undergraduate research symposium that should happen later this semester. In any case I don't mind if this is not fitting for the Algebra seminar, and was just curious since Recep encouraged me to ask anyways. Thanks!