Mathematics GU4042
Introduction to Modern Algebra II

Answers to Practice Midterm #2

April 13, 2017

1. A polynomial is separable if its roots in one (and hence every) splitting field are all distinct. A field extension E/F is separable if the minimal polynomial in $F[x]$ of every element of E is a separable polynomial.

2. $3^{1/7}$ is not constructible, for it is a root of $x^7 - 3$, which is irreducible by Eisenstein and hence is its minimal polynomial over $\mathbb{Q}$. Hence $[\mathbb{Q}(3^{1/7}) : \mathbb{Q}] = 7$, so by multiplicativity $3^{1/7}$ cannot be in any field extension of $\mathbb{Q}$ whose degree is a power of 2. On the other hand, $3^{1/2^{n+1}}$ has minimal polynomial $x^2 - 3^{1/2^n}$ over $\mathbb{Q}(3^{1/2^n})$, so $\mathbb{Q}(3^{1/8})/\mathbb{Q}(3^{1/4})/\mathbb{Q}(3^{1/2})/\mathbb{Q}$ is a tower of quadratic extensions. Hence $3^{1/8}$ is constructible.

3. Since r is algebraic, $\mathbb{Q}(r) = \mathbb{Q}[r]$ and $[\mathbb{Q}(r) : \mathbb{Q}] = p$, the degree of the minimal polynomial. If E is an intermediate field, by multiplicativity $[\mathbb{Q}(r) : E]\,[E : \mathbb{Q}] = p$, so one factor is 1, hence $\mathbb{Q}(r) = E$ or $E = \mathbb{Q}$.

4. Yes. We proved on A7#2 that any splitting field is a finite extension (indeed $[E : F] \leq n!$ for a degree n polynomial). If $\#F = q$ and $[E : F] = k$, then $E \cong F^k$ as a vector space over F, so $\#E = \#F^k = q^k < \infty$.

5. True. Plugging in 0 and 1 shows that neither polynomial has a root, so as cubic polynomials they must be irreducible, so the ideals are maximal, so the quotient rings are fields. The degrees of the extensions of $\mathbb{F}_2$ are both 3, so each has $2^3 = 8$ elements, and we proved that any two finite fields with the same number of elements are isomorphic.

6. Let $\sigma : E \to E$ be $\sigma(z) = \overline{z}$. Then $G = \{\mathrm{id}, \sigma\}$ is a subgroup of Aut E, and $E^G = F$. By the equivalent conditions to be a Galois extension, E/F is finite, normal, and separable. Alternative: if a monic irreducible $f(x) \in F[x]$ has a root $r \in E$, then $\overline{r} \in E$ is also a root, so $(x - r)(x - \overline{r}) \mid f(x)$, but $(x - r)(x - \overline{r}) \in F[x]$ since $r + \overline{r}$ and $r\overline{r}$ are real. Since f is monic and irreducible, $(x - r)(x - \overline{r}) = f(x)$, which therefore splits. Thus E/F satisfies the definition of a normal extension.

7. (a) Reducible as $(x + 1)(x^4 - x^3 + x^2 - x + 1)$; latter is $c_5(-x)$, hence irreducible. If $r = e^{2\pi i/10}$, then roots of $c_5(-x)$ are r, r^3, r^7, r^9; since $E = \mathbb{Q}(r)$ contains all roots, it is the splitting field, and there exists $\phi \in$ Gal taking r to any root. Hence Gal $= \{[1], [3], [7], [9]\} \subset \mathbb{Z}_{10}^\times$ and $3^2 \equiv 9, 3^3 \equiv 7, 3^4 \equiv 1 \pmod{10}$, so Gal $\cong \mathbb{Z}_4$.

(b) Irreducible by Eisenstein, so separable since characteristic is 0, so 3 roots. One root $r \in \mathbb{R}$, others aren't, so real part $\mathbb{Q}(r)$ is a proper subfield of degree 3 over $\mathbb{Q}$. So splitting field has degree 6, hence Gal has 6 elements. Injects into Σ_3, so must be Σ_3.

(c) Factors as $(x^2 - 3)(x^2 + 3)$, so roots are $\pm\sqrt{3}$ and $\pm\sqrt{-3}$. So $E = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ and we know that biquadratic extensions have Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$.