# Solutions to Sample Test

October, 2024

1. (a) The sixth roots of unity are roots of $x^6-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. Here
   - $x-1$ has as its root the primitive first root of unity, 1;
   - $x+1$ has as its root the primitive square root of unity, $\zeta^3 = -1$;
   - $x^2+x+1$ has as its roots the primitive cube roots of unity, $\zeta^2$ and $\zeta^4$; and
   - $x^2-x+1$ has as its roots the primitive sixth roots of unity, $\zeta$ and $\zeta^5=\zeta^{-1}=\overline{\zeta}$.

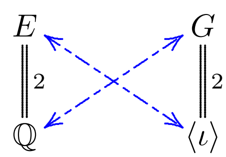
   Of course the roots of $m(x)$ are $\frac{1\pm\sqrt{-3}}{2}$ which are irrational, so $m(x)$ is irreducible in $\mathbb{Q}[x]$.

   (b) We have $[E:\mathbb{Q}] = \deg m(x) = 2$. One explicit choice of basis for $E$ over $\mathbb{Q}$ is $\{1,\zeta\}$; another is $\{1,\sqrt{-3}\}$.

   (c) The nontrivial automorphism of $E$ is complex conjugation, $\tau(x) = \overline{z}$, which interchanges the two roots of $m(x)$. Of course, $G = \langle\tau\rangle = \{\iota,\tau\}$ is the group of order 2; so it is both cyclic and abelian.

   (d) From $\zeta = e^{\pi i/3} = \frac{1}{2}(1+\sqrt{-3})$ we get $\sqrt{-3} = 2\zeta-1 \in E$.

   (e) The blue arrows indicate the Galois correspondence:




2. Given $h \in G$, left-multiplication by $h$ defines a map $G \to G$, $g \mapsto hg$ which is bijective. This map permutes the terms in the sum $T(\alpha)$, so it fixes the sum. Similarly, it permutes the factors in the product $N(\alpha)$, thereby fixing the product. Less verbosely,
$$h(T(\alpha)) = h\Big(\sum_{g\in G} g(\alpha)\Big) = \sum_{g\in G} hg(\alpha) = \sum_{g'\in G} g'(\alpha) = T(\alpha)$$
and
$$h(N(\alpha)) = h\Big(\prod_{g\in G} g(\alpha)\Big) = \prod_{g\in G} hg(\alpha) = \prod_{g'\in G} g'(\alpha) = N(\alpha).$$
Since $T(\alpha)$ and $N(\alpha)$ are fixed by every element $h \in G$, they lie in the fixed subfield of $G$, which is $\mathbb{Q}$ (by the Galois correspondence).

3. Since $\alpha$ is a root of $f(x)$, $2\alpha+1$ is a root of $f\big(\frac{x-1}{2}\big) = \frac{1}{8}m(x)$ where $m(x) = x^3+3x^2-5x+9$. So $m(x)$ is the minimal polynomial of $2\alpha+1$ over $\mathbb{Q}$.

   The irreducibility of $m(x)$ follows directly from the irreducibility of $f(x)$. (Because the change of variable $x \mapsto \frac{x-1}{2}$ is invertible, factoring $m(x)$ in $\mathbb{Q}[x]$ would be equivalent to factoring $f(x)$ in $\mathbb{Q}[x]$.) Alternatively, the irreducibility of $m(x)$ in $\mathbb{Q}[x]$ follows directly from the fact that $m(\pm 1) \neq 0$, so $m(x)$ has no roots in $\mathbb{Z}$, so it has no roots in $\mathbb{Q}$.)

4. one-to-one, subring, nonzero, unit, field, inverse

5. (a) T (b) F (c) T (d) F (e) T (f) T (g) T (h) F (i) T (j) F

   Some comments and explanations, provided for your benefit only (not required for answering #5):

   (a) Every subfield of $\mathbb{R}$ contains $\mathbb{Q}$.

   (b) Consider the extension $E \supset \mathbb{C}$ given by the field $E = \mathbb{C}(x)$ of rational functions in an indeterminate $x$, with complex coefficients. Here $[E : \mathbb{C}] = \infty$.

   (c) This is easy to prove, directly from the axioms.

   (d) If $\alpha = 2^{\frac{1}{3}}$ then $F = \mathbb{Q}[\alpha]$ is an extension of $\mathbb{Q}$ of degree 3, with only one automorphism (the identity). Know your examples.

   (e) Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis for $F$ over $\mathbb{Q}$, and let $\{\beta_1, \ldots, \beta_n\}$ be a basis for $F'$ over $\mathbb{Q}$. Then the set of all products $\alpha_i\beta_j$ spans an extension field $E \supseteq \mathbb{Q}$ containing both $F$ and $F'$. This is an exercise, and we note that $[E : \mathbb{Q}] \leqslant mn$ so $E$ is a finite extension of $\mathbb{Q}$. This looks very much like the proof of transitivity of degrees for field extensions; but we have only the inequality '$\leqslant mn$' here since the products $\alpha_i\beta_j$ are not necessarily linearly independent over $\mathbb{Q}$ in this case. (For examples with inequality, consider for example the case when $F' = F$ is a proper extension of $\mathbb{Q}$.)

   (f) Since $\alpha = \frac{1 \pm \sqrt{13}}{2} \in \mathbb{Q}[\sqrt{13}]$, we have $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{13}]$. The reverse inclusion follows just as easily since $\sqrt{13} = \pm(-1+2\alpha) \in \mathbb{Q}[\alpha]$ implies $\mathbb{Q}[\sqrt{13}] \subseteq \mathbb{Q}[\alpha]$.

   (g) As discussed in class (I think it was Oct 16).

   (h) It is easy to find elements of $S$ that do not commute, e.g. $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$.

   (i) Consider the extension $E = \mathbb{Q}[2^{1/n}] \supseteq \mathbb{Q}$ of degree $[E : \mathbb{Q}] = n$, noting that the polynomial $x^n - 2$ is irreducible in $\mathbb{Q}[x]$.

   (j) Consider the splitting field $E \supset \mathbb{Q}$ of $x^3 - 2$, an extension of degree 6 whose automorphism group is $G \cong S_3$, the symmetric group of degree 3. Recall that one of the three elements of order 2 in $G$ is complex conjugation; and this does not commute with the rest of $G$. Know your examples.