Solution Set 12

Math 123
May 7, 2002

1. *Artin §14.2 #2*

a) Let $f(x) = x^3 - 2$. Eisenstein's criterion ($p = 2$) shows that f is irreducible. The discriminant D is $-27 \cdot 4 < 0$ which is not a square in $\mathbf{Q}$, so the Galois group of f must be S_3.

b) Let $f(x) = x^3 + 27x - 4$. If f were not irreducible then since it is a monic integer cubic with constant term 4, it would have to have ± 1, ± 2, or ± 4 as a root, which it does not. The discriminant is $-4 \cdot 27^3 - 27 \cdot (-4)^2 < 0$, so as above, the Galois group of f is S_3.

---

2. *Artin §14.2 #3*

Let $D = \delta^2$ be the descriminant of f. If $\delta \in F$ then $F = F(\delta)$, so f is irreducible over $F(\delta)$; thus we can assume that $\delta \notin F$. Since $[F(\delta) : F] = 2$ and $[F(\alpha) : F] = 3$ for any root α of f, we know that no root of f is contained in $F(\delta)$; thus since f is cubic we have that f is irreducible over $F(\delta)$.

---

3. *Artin §14.2 #6*

Let $\alpha \in \mathbf{R}$ be the real root of f, and let $\beta, \bar{\beta}$ be the complex roots. We know that the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$ since f is an irreducible cubic, and that $\beta, \bar{\beta} \notin \mathbf{Q}(\alpha)$. Thus $(x - \beta)(x - \bar{\beta})$ is irreducible over $\mathbf{Q}(\alpha)$, so the degree of $K = \mathbf{Q}(\alpha, \beta)$ over $\mathbf{Q}$ is $2 \cdot 3 = 6$.

---

4. *Artin §14.5 #8*

Using the primitive element theorem, assume that $K = F(\alpha)$ and $F' = F(\beta)$, so

$$K' = F(\alpha, \beta) = F(\beta, \alpha) = F'(\alpha).$$

Let f be the minimal polynomial for α over F, and let $G = \mathrm{Gal}(K/F)$. We know that f splits over K since K/F is Galois and any polynomial with a root in a Galois extension splits. Thus f splits over $K' \supset K$ as well, and since $K' = F'(\alpha)$ and $f(x) \in F'[x]$, we have that K' is the splitting field for f over F', so K'/F' is Galois.

Let $G' = \mathrm{Gal}(K'/F')$, and note that any element of G or G' is determined by how it acts on α. Clearly any element g' of G' fixes $F \subset F'$, and since g' takes α to another root of f,

g' stabilizes K. Thus $g'|_K \in G$, so we have a map $\varphi : G' \to G$ taking $g' \mapsto g'|_K$. This map is injective since g' is the identity if and only if g' fixes α, which happens exactly when $g'|_K$ is the identity.

---

5. *Artin §14.5 #9*

a) If K/F is Galois that K is the splitting field of some $f(x) \in F[x]$. But since $F \subset L$, we have that K is the splitting field of $f(x) \in L[x]$ too, so K/L is Galois.

b) Let $F = \mathbf{Q}$ and let $f(x) = x^3 - 2$. Then f has exactly one real root α. Let $L = F(\alpha)$ and let K be the splitting field of f. Thus K/F is Galois, but since the complex roots of f are not contained in L, L/F is not Galois (since a polynomial with a root in a Galois extension splits).

c) Let $F = \mathbf{Q}$, $L = F(\sqrt{2})$, and $K = L(\sqrt[4]{2})$, so $F \subset L \subset K \subset \mathbf{R}$. Since any degree 2 extension is Galois, we know that K/L and L/F are both Galois. However, the irreducible polynomial (by Eisenstein) $f(x) = x^4 - 2 \in F[x]$ has a root in K but does not split in K since f has the complex root $i\sqrt[4]{2}$, so K/F is not Galois.

---

6. *Artin §14.5 #11*

It is true that K/F is the splitting field of an irreducible cubic. Let $G = \mathrm{Gal}(K/F) \cong S_3$, and let $H < G$ be a subgroup of order 2 (e.g. $\{1, (12)\}$) with corresponding intermediate field $L = K^H$. Note that since L is not Galois over F since H is not normal in G. Since K/L is Galois with Galois group H, we have $[K : L] = 2$ which means $[L : F] = 3$. Let $\alpha \in L$ be a primitive element over F, with minimal polynomial $f(x) \in F[x]$. We know that f does not split over L since L/F is not Galois, but that f does split over K since K/F is Galois. Thus K is the splitting field of the irreducible cubic f.

A common error in this problem was to say, "K/F is the splitting field of *some* polynomial; we just have to prove that this polynomial has an irreducible cubic factor." This is false. Note that by the primitive element theorem, *any* degree six Galois extension is the splitting field of an irreducible sextic.

---

7. *Artin §14.9 #1*

Note: contrary to popular belief, one cannot solve this problem "by inspection." It is quite tedious to give the subgroups and prove that there are no others.

Let $G = S_5$. First note that since a transitive subgroup H has to send the letter 1 to each other letter, it must have order at least 5. Also, since H acts on the set $\{1, 2, 3, 4, 5\}$ by permutations, we can use the stabilizer-orbit formula to conclude that the order of H is

a multiple of 5 (since the size of the orbit of 1, say, is always 5). Since $|S_3| = 120$, then, we find that $|H| \in \{5, 10, 15, 20, 30, 40, 60, 120\}$. We will proceed by finding all transitive subgroups (up to conjugation, a.k.a. relabelling of the letters) of each order.

- $|H| = 5$. Thus $H \cong C_5$. The only elements of order 5 in S_5 are 5-cycles, so H is conjugate to $\langle(12345)\rangle$.

- $|H| = 10$. The Sylow theorems tell us that H contains a subgroup of order 5, say $\sigma = (12345)$. The stabilizer of any element will be a subgroup of order 2. Since S_5 is generated by any five-cycle and transposition, we know that the stabilizer of 1, for instance, must be a double transposition, i.e. it is either $(23)(45)$, $(24)(35)$, or $(25)(34)$. Now, $(12345)(23)(45) = (135)$ which has order three and is not in H, so $(23)(45) \notin H$. Also $(12345)(24)(35) = (14325) \notin \langle(12345)\rangle$, so H would have to have two subgroups of order 5, which is impossible by the Sylow theorems. Thus $\tau = (25)(34) \in H$; note that $\sigma\tau = \tau\sigma^{-1}$ Since $|H| = 5 \cdot 2$, we have $H = \langle\sigma\rangle\langle\tau\rangle$, so we can write

  $$H = \langle\sigma, \tau;\ \sigma^5, \tau^2, \sigma\tau = \tau\sigma^{-1}\rangle$$

  so $H \cong D_5$. Note that D_5 can be realized more concretely as a subgroup of S_5 as the action of the symmetries of a pentagon on its vertices.

- $|H| = 15$. We know that every group of order 15 is cyclic (cf. Artin Proposition 6.4.9). But S_5 contains no element of order 15, so there is no subgroup of S_5 of order 15.

- $|H| = 20$. The Sylow theorems tell us that there is a normal subgroup of order 5, so as usual we can assume that $(12345) \in H$. Let G_1 be the stabilizer of the letter 1; note that $|G_1| = 4$. We claim that G_1 is cyclic. Suppose not, so G_1 is isomorphic to the Klein four group. Since H does not contain a transposition (it contains a 5-cycle), G_1 must contain three double transpositions, so $G_1 = \{1, (23)(45), (24)(35), (25)(34)\}$. But as before, $(12345)(23)(45) = (135)$ has order 3 which does not divide 20, a contradiction.

  Let $K = \langle(12345)\rangle$. Since $K \cap G_1 = \{1\}$ by comparing orders of elements, and $|K||G_1| = |H|$, we have $KG_1 = H$, so H is generated by (12345) and a generator of K. Now we only have three cases to check, since there are six elements of order four in $S_4 \supset G_1$, and two are generators of each choice of G_1. Well, $(12345)(2345) = (135)(24)$ which has order six and is thus not in H, so $G_1 \neq \langle(2345)\rangle$. Also, $(2435)(12345)(2534) = (15423) \notin K$, which is bad since K is normal; thus $G_1 \neq \langle(2435)\rangle$. The only remaining possibility is $G_1 = \langle(2354)\rangle$. Letting $\sigma = (12345), \tau = (2354)$, then, we have

  $$H = \langle\sigma, \tau;\ \sigma^5, \tau^4, \tau\sigma = \sigma^3\tau\rangle$$

  (this is a complete presentation since we know $\tau\sigma\tau^{-1}$). This is indeed a group of order 20, as it is isomorphic to the semidirect product $C_4 \ltimes C_5$ with the action of C_4 on C_5 coming from the isomorphism $C_4 \cong (\mathbf{Z}/5\mathbf{Z})^* \cong \operatorname{Aut} C_5$ sending a generator of C_4 to the automorphism $x \mapsto x^3 : C_5 \to C_5$.

- $|H| = 30$. The Sylow theorems tell us that we have one or six subgroups of order five. Suppose that there were six subgroups of order five. Since their intersections must be trivial, that accounts for 24 of the non-identity elements. Now, the stabilizer of any letter must have order six, so that accounts for the other five non-identity elements of H. But this means that each element is stabilized by the same subgroup, which is a

contradiction since the only element of S_5 that stabilizes all five letters is the identity. Thus there is only one subgroup K of five elements; we can assume that K is generated by (12345).

Now, we have 1 or 10 subgroups of order 3; we must have 10 because we cannot have a normal subgroup of order 3 because that would yield an element of order 15. However, there are only $2 \cdot \binom{5}{2} = 20$ elements of order 3 in S_5, so H must contain all of them. In particular, $(123) \in H$. But $(123)(12345)(321) = (12453) \notin K$, a contradiction. Thus there is no transitive subgroup of order 30.

- $|H| = 40$. The stabilizer $G_5 \subset S_4$ of the letter 5 has order 8; we claim that G_5 acts transitively on $\{1, 2, 3, 4\}$. Suppose not. Thus G_5 contains no element of order four, so it is made up entirely of single and double transpositions. But Sylow theory tells us that H has a subgroup of order 5, so we can assume that $(12345) \in H$; therefore G_5 can contain no single transposition (because a 5-cycle and a transposition generates S_5). Thus G_5 contains the identity and seven double transpositions, a contradiction since S_4 only has three double transpositions. Thus G_5 is a transitive subgroup of S_4. By Artin, 14.6.11, the only transitive subgroup of S_4 of order 8 is D_4. But D_4 contains two single transpositions (flipping about the diagonal of the square), a contradiction. Therefore there is no transitive subgroup of order 40.

- $|H| = 60$. The only subgroup of S_5 of order 60 is A_5 by Jordan-Hölder, since A_5 is simple.

- $|H| = 120$, i.e. $H = S_5$.

Therefore the possible subgroups are isomorphic to $C_5, D_5, C_4 \ltimes C_5, A_5$, and S_5, with the embeddings given above.

---

8. *Artin §14.9 #2*

This follows from the previous problem, since the only transitive subgroups of S_5 whose order is a multiple of 3 are A_5 and S_5.

---

9. *Artin §14.9 #7*

Recall (Artin Theorem 13.4.9) that an element α can be constructed by ruler and compass if and only if there is a tower of field extensions

$$\mathbf{Q} = F_1 \subset F_2 \subset \cdots \subset F_n \tag{1}$$

with $[F_i : F_{i-1}] = 2$ for each i and $F_n = F_{n-1}(\alpha)$. Note that it is *not* necessarily true that each $F_i \subset \mathbf{Q}(\alpha)$, or that $[F_n : \mathbf{Q}] = 4$.[1]

[1] This was a common error. Re-read the definitions.

Now let $\alpha \in \mathbf{R}$ have minimal polynomial $f(x) \in \mathbf{Q}[x]$ of degree 4, and let $G = \mathrm{Gal}(f/\mathbf{Q})$. G is thus a transitive subgroup of S_4, so it is one of the groups listed in Artin 14.6.11, namely S_4, A_4, D_4, C_4, or the Klein four group V. Let $K/\mathbf{Q}$ be the splitting field of f; suppose that $f(x) = \prod_{i=1}^{4}(x - \alpha_i)$ in K, where $\alpha = \alpha_1$.

CLAIM 9.1. *α is constructible $\iff$ $G = D_4, C_4$, or V.*

PROOF.

($\Longrightarrow$) We will show that if $G = S_4$ or A_4 then α is not constructible. Suppose the contrary, that α is constructible. Let $F = F_{n-1}$, so $F_n = F(\alpha)$. Thus the minimal polynomial g for α over F has degree two; suppose without loss of generality that $g(x) = (x - \alpha_1)(x - \alpha_2)$. Thus $g(0) = \alpha_1\alpha_2 \in F$, and since $f(x)/g(x) \in F$, we know that $\alpha_3\alpha_4 \in F$. Thus $\beta = \alpha_1\alpha_2 + \alpha_3\alpha_4 \in F$. Now, as in Artin p.563, the orbit of β under $A_4 \subseteq G$ is

$$\{\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \;\; \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \;\; \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3\}$$

(since $(234) \in A_4$). We should note that no two β_i are the same, since for instance,

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \iff \alpha_1(\alpha_2 - \alpha_3) = \alpha_4(\alpha_2 - \alpha_3)$$

which is a contradiction since f has distinct roots (since $\mathbf{Q}$ has characteristic zero and f is irreducible). Therefore β has degree three over $\mathbf{Q}$. But $\mathbf{Q}(\beta) \subset F$, so

$$[F : \mathbf{Q}] = [F : \mathbf{Q}(\beta)][\mathbf{Q}(\beta) : \mathbf{Q}]$$

is a multiple of three, which contradicts the fact that $[F : \mathbf{Q}]$ is a power of 2 (since F is in a tower (1) of square roots). Thus α is not constructible.

($\Longleftarrow$) Suppose that $G = D_4, C_4$, or V. It suffices to find a proper intermediate extension L between $\mathbf{Q}$ and $\mathbf{Q}(\alpha)$, since then

$$\mathbf{Q} \subsetneq L \subsetneq \mathbf{Q}(\alpha)$$

would be a tower of degree two extensions. Now, if $G = C_4$ or V then $K = \mathbf{Q}(\alpha)$ is the splitting field, and any order two subgroup of G will have a fixed field L which satisfies our requirements.

If $G = D_4$ then $[K : \mathbf{Q}(\alpha)] = 2$, so $G' = \mathrm{Gal}(K/\mathbf{Q}(\alpha))$ is a subgroup of order two; since G' permutes the α_i and fixes $\alpha = \alpha_1$, G' must be generated by a transposition, say $G' = \langle(\alpha_3, \alpha_4)\rangle$. We would like to find a subgroup H of order 4 that contains G', so that $L = K^H$ is a field contained in $\mathbf{Q}(\alpha)$ with $[K : L] = 4 \implies [\mathbf{Q}(\alpha) : L] = 2$. Well, if $(\alpha_3, \alpha_4) \in G$ then $(\alpha_1, \alpha_2) \in G$ (remember the embedding of D_4 into S_4 consisting of the action on the vertices of the symmetries of a square), so the subgroup $H = \{1, (12), (34), (12)(34)\}$ will do. Thus α is constructible.

❐