Mathematics 352 – Abstract Algebra II
Solutions for Problem Set 7
March 25, 2008

Chapter 15

7. We must have $x^2y = 3$ from the volume constraint and $2x^2 + 4xy = 7$ from the surface area constraint. Solving for x in the first equation, $y = \frac{3}{x^2}$. So then in the second equation $2x^2 + \frac{12x}{x^2} = 7$, or $2x^3 - 7x + 12 = 0$. By the rational roots test, the possible rational roots of this polynomial equation are $x = \pm 1, 2, 3, 4, 6, 12, \frac{1}{2}, \frac{3}{2}$. But it is easy to check that none of these are roots. This implies that $f(x) = 2x^3 - 7x + 12$ is irreducible in $\mathbb{Q}[x]$. Therefore, $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, so x is not constructible by Theorem 15.9 in the text, or the Corollary of the main theorem on constructible numbers we stated in class: $[\mathbb{Q}(x) : \mathbb{Q}]$ is not a power of 2.

8. Use Theorem 15.1. A segment of length $\sqrt{3}$ can be constructed by this process:

- construct a semicircle of diameter 4 – call the end points A, B,
- erecting a perpendicular to the diameter at a point C dividing the diameter into lengths $AC = 1, CB = 3$ and
- find the intersection of D the perpendicular with the semicircle (see diagram on page 454 or a slightly different diagram in the class notes).

Then given the segment $\overline{CD}$ of length $\sqrt{3}$, construct a circle with center C and radius $CD = \sqrt{3}$. This intersects the line containing the diameter of the semicircle at E, and $AE = 1 + \sqrt{3}$. (There are several other correct method here too.)

9. The answer is *no*. Call the sides of the triangle x, y (where x is the length of the two equal sides). Then the perimeter is $2x + y = 8$. Taking the side of length y as the base, and using the Pythagorean theorem, the area is $1 = \frac{1}{2}y\sqrt{x^2 - \frac{y^2}{4}}$, which implies, after squaring and rearranging,

$$4x^2y^2 - y^4 = 16.$$

Now from the perimeter equation, $y = 8 - 2x$, so

$$4x^2(8 - 2x)^2 - (8 - 2x)^4 = 16,$$

which implies

$$8x^3 - 80x^2 + 256x - 257 = 0.$$

This cubic is irreducible in $\mathbb{Q}[x]$, since it has no rational roots. Therefore, $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, so x is not a constructible number.

11. Consider the unit circle centered at $(0, 0)$. An angle of t degrees is constructible if and only if we can construct a line ℓ meeting the x-axis at an angle of t degrees (measured counterclockwise

from the positive x-axis). That line intersects the unit circle at the points $\pm(\cos(t), \sin(t))$. Hence the angle is constructible if and only if $\cos(t)$ is a constructible number by the definition (see page 453 in the text, or the class notes).

17. As given in the Hint, the case where C is on the line L is done in the text. If C is not in L, let D be any constructible point on L (there must be such points D since it is given that L is constructible). Using the compass, construct the circle Γ with center at C and radius $\overline{CD}$. The circle Γ intersects L either in

- Two points D, E, or
- In just one point D.

In the second case, L is tangent to Γ at D, and we claim that the tangent L must be perpendicular to the radius $\overline{CD}$ so we are done. This is a standard geometric fact; it can be proved most easily by parametrizing the circle and computing the tangent line from the parametric equations. (A strictly Euclidean proof without using the idea of reflection across the line CD is more difficult, though still possible!)

(Alternately, we can argue that any line must contain (at least) two distinct constructible points. Therefore, there must be some point D such that the circle with radius $\overline{CD}$ is not tangent to L.)

In the first case, construct the circles Γ_1 with center D and radius DC, and Γ_2 with center E and radius EC. The circles Γ_1 and Γ_2 meet at the constructible points C and Q. We claim that $\overline{CQ} \perp \overline{DE}$, so extending the line $\overline{CQ}$ gives the line we are looking for. First, we have $CD = CE$ since both are radii of the same circle. Similarly, $CD = DQ$ and $CE = EQ$. This implies that ΔCDE is isosceles, so $\angle CDE = \angle CED$. Similarly $\angle QDE = \angle QED$. Hence

$$\angle QDE + \angle EDC = \angle QDC = \angle QEC = \angle QED + \angle DEC.$$

From this, we see that $\Delta CDQ \cong \Delta CEQ$ by the SAS congruence theorem. Call S the intersection point of the lines $\overline{DE}$ and $\overline{CQ}$. By the triangle congruence $\Delta CDQ \cong \Delta CEQ$ above, $\angle DCS = \angle ECS$. This implies $\Delta DCS \cong \Delta ECS$ (by SAS again, since $CD = CE$ and CS is in both triangles). Hence $\angle DSC$ and $\angle ESC$ are right angles since they are equal and add up to a straight angle (i.e. $180°$). Thus $\overline{CQ} \perp \overline{DE}$, which is what we wanted to show.

19. Let A be a constructible point not on the constructible line L. By Exercise 17, we can construct a line M through A perpendicular to L. Then using the example from the text on page 451, we can construct a line N passing through A that is perpendicular to M. Since the L and N are both perpendicular to M, but they meet M at different points (one at A, one at a point different from A), L and M must be parallel.

Section 11.1

2. Yes this is true. If $\{v_1, \ldots, v_n\}$ is a basis for K over F, then each $a \in K$ is uniquely $a = c_1v_1 + \cdots + c_nv_n$ for $c_1, \ldots, c_n \in F$. Suppose ϕ, ψ are two F-automorphisms of K such that

$\phi(v_i) = \psi(v_i)$ for all $i = 1, \ldots, n$. Then for each $a \in K$,

$$\begin{aligned}
\phi(a) &= \phi(c_1v_1 + \cdots + c_nv_n) \\
&= c_1\phi(v_1) + \cdots + c_n\phi(v_n) \quad \text{since } \phi \text{ is an } F\text{-automorphism of } K \\
&= c_1\psi(v_1) + \cdots + c_n\psi(v_n) \quad \text{by assumption} \\
&= \psi(c_1v_1 + \cdots + c_nv_n) \quad \text{since } \psi \text{ is an } F\text{-automorphism of } K \\
&= \psi(a).
\end{aligned}$$

In other words, F-automorphisms are completely determined by their action on a basis of K over F.

3. We are given that $\sigma \in \mathrm{Gal}_F(K)$, so σ is an F-automorphism of K. If $u \in K$ satisfies $\sigma(u) = u$, then we claim that $\sigma(a) = a$ for all $a \in F(u)$. This will suffice to show that $\sigma \in \mathrm{Gal}_{F(u)}(K)$ since by definition, elements of $\mathrm{Gal}_{F(u)}(K)$ are automorphisms of K fixing all the elements of $F(u)$. Now we are given that $[K : F]$ is finite. since $F \subseteq F(u) \subseteq K$, by Theorem 10.4,

$$[K : F] = [K : F(u)][F(u) : F]$$

and hence $[F(u) : F]$ is finite as well. Theorem 10.7 implies that if $[F(u) : F] = n$, then $1, u, \ldots, u^{n-1}$ is a basis for $F(u)$ over F. Hence if $a \in F(u)$, then $a = c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$ for some $c_i \in F$. But then as in the previous exercise,

$$\begin{aligned}
\sigma(a) &= \sigma(c_0 + c_1u + \cdots + c_{n-1}u^{n-1}) \\
&= c_0 + c_1\sigma(u) + \cdots + c_{n-1}(\sigma(u))^{n-1} \quad \text{since } \sigma \text{ is an } F\text{-automorphism of } K \\
&= c_0 + c_1u + \cdots + c_{n-1}u^{n-1} \quad \text{since } \sigma(u) = u \\
&= a.
\end{aligned}$$

Thus $\sigma(a) = a$ for all $a \in F(u)$.

8. The mapping $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ defined by $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$ (that is

$$\sigma(a_0 + a_1\sqrt[4]{2} + a_2\sqrt{2} + a_3(\sqrt[4]{2})^3) = a_0 - a_1\sqrt[4]{2} + a_2\sqrt{2} - a_3(\sqrt[4]{2})^3$$

is also an element of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))$. This is true since σ fixes all $a_0 \in \mathbb{Q}$, and if $a = a_0 + a_1\sqrt[4]{2} + a_2\sqrt{2} + a_3(\sqrt[4]{2})^3$ and $b = b_0 + b_1\sqrt[4]{2} + b_2\sqrt{2} + b_3(\sqrt[4]{2})^3$, then

$$\begin{aligned}
\sigma(a + b) &= \sigma((a_0 + b_0) + (a_1 + b_1)\sqrt[4]{2} + (a_2 + b_2)\sqrt{2} + (a_3 + b_3)(\sqrt[4]{2}^3)) \\
&= (a_0 + b_0) - (a_1 + b_1)\sqrt[4]{2} + (a_2 + b_2)\sqrt{2} - (a_3 + b_3)(\sqrt[4]{2}^3 \\
&= (a_0 - a_1\sqrt[4]{2} + a_2\sqrt{2} - a_3(\sqrt[4]{2})^3) + (b_0 - b_1\sqrt[4]{2} + b_2\sqrt{2} + b_3(\sqrt[4]{2})^3) \\
&= \sigma(a) + \sigma(b).
\end{aligned}$$

Moreover,

$$\begin{aligned}
\sigma(ab) &= \sigma\Big((a_0b_0 + 2a_1b_3 + 2a_2b_2 + 2a_3b_1) + (a_0b_1 + a_1b_0 + 2a_2b_3 + 2a_3b_2)\sqrt[4]{2} \\
&\quad + (a_0b_2 + a_2b_0 + a_1b_1 + 2a_3b_3)\sqrt{2} + (a_0b_3 + a_3b_0 + a_1b_2 + a_2b_1)(\sqrt[4]{2}^3)\Big) \\
&= (a_0b_0 + 2a_1b_3 + 2a_2b_2 + 2a_3b_1) - (a_0b_1 + a_1b_0 + 2a_2b_3 + 2a_3b_2)\sqrt[4]{2} \\
&\quad +(a_0b_2 + a_2b_0 + a_1b_1 + 2a_3b_3)\sqrt{2} - (a_0b_3 + a_3b_0 + a_1b_2 + a_2b_1)(\sqrt[4]{2}^3) \\
&= (a_0 - a_1\sqrt[4]{2} + a_2\sqrt{2} - a_3(\sqrt[4]{2})^3)\cdot(b_0 - b_1\sqrt[4]{2} + b_2\sqrt{2} + b_3(\sqrt[4]{2})^3) \\
&= \sigma(a)\sigma(b).
\end{aligned}$$

Therefore σ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[4]{2})$.

9. (a) Since $x^3-1=(x-1)(x^2+x+1)$ in $\mathbb{Q}[x]$, the minimal polynomial of $\omega=\frac{-1+i\sqrt{3}}{2}$ is x^2+x+1. By the quadratic formula, the roots of this are

$$x=\frac{-1\pm i\sqrt{3}}{2}.$$

Taking the $+$ sign gives ω, the other root $\frac{-1-i\sqrt{3}}{2}$ equals ω^2,

(b) The Galois group $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))=\{id,\sigma\}$ where $\sigma(\omega)=\omega^2$. This is cyclic of order 2, isomorphic to $\mathbb{Z}_2$. Note that by Theorem 11.3, every $\mathbb{Q}$-automorphism of $\mathbb{Q}(\omega)$ takes ω to either ω or to ω^2.