Math 461 F **Spring 2011**
Homework 4 Solutions **Drew Armstrong**

A.1. Euclid's Lemma. Suppose that a divides bc for $a, b, c \in \mathbb{Z}$ with a and b coprime (i.e. they have no common factor except ± 1). **Prove** that a must divide c. (Hint: Since a and b are coprime, you may assume — without proof — that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.)

Proof. Since a and b are coprime they have greatest common divisor 1. You may have seen in another class the fact that the greatest common divisor of (a, b) is always an integer linear combination of a and b. That is, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Now multiply both sides of this equation by c to get

$$axc + (bc)y = c.$$

By assumption we have $bc = ak$ for some $k \in \mathbb{Z}$, hence

$$axc + (bc)y = axc + aky = a(xc + ky) = c.$$

In other words, a divides c. □

A.2. Prove that $\sqrt[3]{2}$ is not rational.

Proof. Suppose for contradiction that $\sqrt[3]{2}$ is rational. Then we can write $\sqrt[3]{2} = a/b$ as a fraction in lowst terms (i.e. $a, b \in \mathbb{Z}$ with a, b coprime). Cubing both sides of this equation gives $2 = a^3/b^3$, or $a^3 = 2b^3$. Since a^3 is even we may conclude that a is even (for if a were odd then a^3 would be odd), and we write $a = 2k$ for some $k \in \mathbb{Z}$. But then we have $2b^3 = a^3 = 8a^3$, or $b^3 = 4a^3$, which implies that b^3, and hence b, is even. We have found that a and b are both even, which contradicts the assumption that they are coprime. Hence $\sqrt[3]{2}$ is not rational. □

A.3. Consider a quadratic field extension $F \subseteq F[\sqrt{c}] = \{a + b\sqrt{c} : a, b \in F\}$ and define the conjugation map $a + b\sqrt{c} \mapsto a - b\sqrt{c}$. **Prove** that for all $u, v \in F[\sqrt{c}]$ we have

- $\overline{u + v} = \overline{u} + \overline{v}$,
- $\overline{uv} = \overline{u}\,\overline{v}$.

Proof. Let $u = a + b\sqrt{c}$ and $v = d + e\sqrt{c}$. Then we have

$$\begin{aligned}
\overline{(a + b\sqrt{c}) + (d + e\sqrt{c})} &= \overline{(a + d) + (b + e)\sqrt{c}} \\
&= (a + d) - (b + e)\sqrt{c} \\
&= (a - b\sqrt{c}) + (d - e\sqrt{c}) \\
&= \left(\overline{a + b\sqrt{c}}\right) + \left(\overline{d + e\sqrt{c}}\right)
\end{aligned}$$

and

$$\begin{aligned}\overline{(a+b\sqrt{c})(d+e\sqrt{c})} &= \overline{(ad+cbe)+(ae+bd)\sqrt{c}} \\ &= (ad+cbe)-(ae+bd)\sqrt{c} \\ &= (a-b\sqrt{c}))(d-e\sqrt{c}) \\ &= \left(\overline{a+b\sqrt{c}}\right)\left(\overline{d+e\sqrt{c}}\right).\end{aligned}$$

□

A.4. Consider again the same field extension $F \subseteq F[\sqrt{c}]$ and let $p(x) \in F[x]$ be a polynomial with coefficients in F. Prove that for any $\alpha \in F[\sqrt{c}]$ we have

$$p(\alpha) = 0 \quad \Longleftrightarrow \quad p(\overline{\alpha}) = 0.$$

Proof. First we will prove $\Rightarrow$. Suppose that $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with $a_0, \ldots, a_n \in F$. If $\alpha \in F[\sqrt{c}]$ is a root of $p(x)$ then we have

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Consider the general term $a_i\alpha^i$. Since $a_i \in F$ we have $\overline{a_i} = a_i$ and then the multiplicative property of conjugation (Problem A.3) gives $\overline{a_i\alpha^i} = a_i(\overline{\alpha})^i$. Now conjugate both sides of the equation $p(\alpha) = 0$ to get

$$\begin{aligned}\overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0} &= \overline{0} \\ \overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \cdots + \overline{a_1\alpha} + \overline{a_0} &= 0 \\ a_n(\overline{\alpha})^n + a_{n-1}(\overline{\alpha})^{n-1} + \cdots + a_1\overline{\alpha} + a_0 &= 0.\end{aligned}$$

We conclude that $\overline{\alpha}$ is a root of $p(x)$, as desired.

Next we will prove $\Leftarrow$. Suppose that $\overline{\alpha}$ is a root of $p(x)$. The above argument then shows that the conjugate of $\overline{\alpha}$ is also a root. That is, $\overline{\overline{\alpha}} = \alpha$ is a root, as desired. □

For the next two problems you may assume — without proof — that $2\cos(2\pi/7)$ is a root of $x^3 + x^2 - 2x - 1 = 0$.

Actually, I'll prove this for you. Let $\omega = \cos(2\pi/7) + i\sin(2\pi/7)$, so that

$$\omega^3, \omega^2, \omega, 1, \omega^{-1}, \omega^{-2}, \omega^{-3}$$

are the 7th roots of unity, and hence their sum is 0. We are interested in finding an equation satisfied by $u = \omega + \omega^{-1} = \omega + \overline{\omega} = 2\cos(2\pi/7)$. If we try to obtain the sum of all 7th roots by combining powers of u (working from highest degree inward) we will find that

$$u^3 + u^2 - 2u - 1 = \omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3} = 0,$$

as desired.

A.5. Prove that $x^3 + x^2 - 2x - 1 = 0$ has no rational root, and hence that $\cos(2\pi/7)$ is not rational.

Proof. Suppose that a/b is a rational root in lowest terms (i.e. $a, b \in \mathbb{Z}$ with a, b coprime). Then we have

$$\frac{a^3}{b^3} + \frac{a^2}{b^2} - 2\frac{a}{b} - 1 = 0,$$

or

$$a^3 + a^2 b - 2ab^2 - b^3 = 0.$$

Taking b^3 to the right hand side we find that a divides b^3. But since a and b are coprime this implies that $a = \pm 1$. Similarly, taking a^3 to the right hand side shows that b divides a^3, and hence $b = \pm 1$. That is, the only possible rational roots of our polynomial are $a/b = \pm 1$. We can easily check that neither of these is a root, and hence there are no rational roots.

Since $2\cos(2\pi/7)$ is a root of the polynomial, we conclude that it is not rational. This implies that $\cos(2\pi/7)$ is not rational since, if it were, then $2\cos(2\pi/7)$ would be rational. □

A.6. Prove that $\cos(2\pi/7)$ is not constructible, and hence that the regular heptagon is not constructible with straightedge and compass.

Proof. Let $f(x) = x^3 + x^2 - 2x - 1$ and let $F \subseteq F[\sqrt{c}$ be any quadratic field extension such that $\mathbb{Q} \subseteq F$. We saw in class (and on the handout) that: **if** $f(x)$ has a root in $F[\sqrt{c}]$ **then** it also has a root in F. Now suppose for contradiction that $2\cos(2\pi/7)$ **is** constructible. Then there exists a chain of quadratic extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k$$

such that $2\cos(2\pi/7) \in F_k$. That is, $f(x)$ has a root in F_k. But by the above remark, this implies that $f(x)$ also has a root in F_{k-1}. Repeating this argument k times shows that $f(x)$ has a root in $\mathbb{Q}$ which we showed in Problem A.5 is a contradiction. Hence $2\cos(2\pi/7)$ is **not** constructible.

(You do not need to say anything more, but I'll finish off the argument.) Now suppose that the regular heptagon is constructible with straightedge and compass. Consider the fan of rays from the center of the heptagon through its vertices and intersect this with a unit circle to get a heptagon of "unit radius". We can assume that one of the vertices has coordinates $(1, 0)$ and hence the next vertex counterclockwise has coordinates $(\cos(2\pi/7), \sin(2\pi/7))$. This implies that the number $\cos(2\pi/7)$ and hence the number $2\cos(2\pi/7)$ is constructible, which is a contradiction. Hence the regular heptagon is not constructible. □