18.702 Comments on Problem Set 8

1. Chapter 15, Exercise 5.2. (constructing the regular pentagon)

(a) The problem is to construct the angle $2\pi/5$, which amounts to constructing its cosine. Let $\zeta = e^{2\pi i/5}$. Then $\zeta + \zeta^4 = 2 \cos 2\pi/5$. Let’s write $2 \cos 2\pi/5 = \alpha$. Then $\alpha^2 = \zeta^2 + 2 + \zeta^3$. Using the equation $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$, one finds that $\alpha$ is a root of $x^2 + x - 1$, and $\alpha = (-1 + \sqrt{5})/2$. Since field operations and square roots are available, $\alpha$ can be constructed.

2. Chapter 15, Exercise 3.4. (the irreducible polynomials for some $\zeta$)

We’ll analyze the case of $\zeta_{10}$. To avoid confusion, let’s denote $\zeta_3$ by $\omega$. Also, let’s denote $\mathbb{Q}$ by $F$ and $\mathbb{Q}(\omega)$ by $K$.

It simplifies things a little to note that $\zeta_{10} = -\zeta_5$. The irreducible polynomial for $\zeta_5$ over $F$ is $f(x) = x^4 + x^3 + x^2 + x + 1$, so the irreducible polynomial for $\zeta_{10}$ over $F$ is $f(-x) = x^4 - x^3 + x^2 - x + 1$. Moreover, $f(x)$ will be irreducible over $K = F(\omega)$ if and only if $f(-x)$ is irreducible over $K$. We can work with $\zeta = \zeta_5$.

First, $f$ doesn’t have a root in $K$ because $f(x)$ has degree 4 and $[K:F] = 2$. If $f$ factors in $K[x]$, it must be the product $f = q_1 q_2$ of two quadratic polynomials. The roots of $q_1, q_2$, taken together, will be the roots $\zeta, \zeta^2, \zeta^3, \zeta^4$ of $f$. Let’s say that $\zeta$ is a root of $q_1(x) = x^2 + ax + b$, with $a, b$ in $K$, and let $z'$ be the other root of $q_1$. Then $(x - \zeta)(x - \zeta^4) = x^2 + ax + b$. So $b = \zeta \zeta^4 = \zeta^{i+1}$ must be in $K$. But $\zeta^{i+1}$ has degree 4 over $F$ unless $i + 1 = 5$. The other root must be $\zeta^4 = \zeta^{-1}$. Then $a = \zeta + \zeta^{-1}$. This is a real number in $K$. The real numbers in $K$ are the elements of $F$. So $a$ is a rational number, and $\zeta$ is the root of a quadratic polynomial with rational coefficients. Since $\zeta$ has degree 4 over $F$, this isn’t the case. We conclude that $f$ remains irreducible over $K$.

3. Chapter 15, Exercise 3.7b. (is $\sqrt{5}$ in the field $\mathbb{Q}(\sqrt{2})$?)

I think you will have guessed that the answer is ‘No’. There is an easy way to show this, but we don’t know it yet. We’ll just blast away.

Let $\alpha = \sqrt{2}$ and $\beta = \sqrt{5}$. Also, let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$. The irreducible polynomial for $\alpha$ over $F$ is $x^2 - 2$. So $[K:F] = 3$, and $(1, \alpha, \alpha^2)$ is an $F$-basis for $K$. Can we write $\beta$ in the form $a + b\alpha + c\alpha^2$ with $a, b, c$ in $F$?

We expand $5 = \beta^3 = (a + b\alpha + c\alpha^2)^3$, obtaining

$$5 + 0a + 0\alpha^2 = (a^3 + 2b^3 + 4c^3) + 3(a^2b + 2ac^2 + 2b^2c)\alpha + 3(ab^2 + a^2c + 2bc^2)\alpha^2$$

So we want

$$a^3 + 2b^3 + 4c^3 = 5, \quad a^2b + 2ac^2 + 2b^2c = 0, \quad \text{and} \quad ab^2 + a^2c + 2bc^2 = 0$$

We multiply the second of these equations by $c$, the third by $b$ and subtract. This gives

$$a^2bc + 2ac^3 - ab^3 - a^2bc = a(2c^3 - b^3) = 0$$

We can’t solve $2c^3 - b^3 = 0$ in $\mathbb{Q}$, so $a = 0$. Then the second equation shows that $b = 0$ or $c = 0$, etc.
4. Chapter 15, Exercise M3. (factoring a polynomial of degree 6)

Let $\alpha$ be a root of $f$ in some field extension of $K$. Then $[F(\alpha) : F] = 6$. We have two towers of fields: $F \subset F(\alpha) \subset K(\alpha)$ and $F \subset K \subset K(\alpha)$. So

$$[K(\alpha) : F(\alpha)] [F(\alpha) : F] = [K(\alpha) : F] = [K(\alpha) : K][K : F]$$

Since $K$ is a quadratic extension of $F$, the degree $[K(\alpha) : F(\alpha)]$ is at most 2, and $[F(\alpha) : F] = 4$. So $[K(\alpha) : F]$ can be 6 or 12. Next, we are given that $[K : F] = 2$. So if $[K(\alpha) : F] = 2$, then $[K(\alpha) : K] = 6$, and therefore $f$ remains irreducible over $K$. If $[K(\alpha) : F] = 6$, then $[K(\alpha) : K] = 3$. In this case, the irreducible polynomial for $\alpha$ over $K$ is cubic: $f$ factors in $K[x]$. Since $f$ can’t have a root in $K$, both factors have degree 3.

5. Chapter 15, Exercise M5 (a). (elements of finite order in $GL_2(\mathbb{Z})$)

Let $n$ be an integer and let $A$ be a $2 \times 2$ integer matrix such that $A^n = I$. Then $\det A$ is an integer and $\det A^n = 1$. So $\det A = \pm 1$. Let $\lambda$ be an eigenvalue of $A$. Then $\lambda^n = 1$. The eigenvalues are roots of the characteristic polynomial, and because $A$ is a $2 \times 2$ integer matrix, its characteristic polynomial is a quadratic polynomial $x^2 + sx \pm 1$, with integer $s$, the trace of $A$.

My hope was that you would determine the integers $n$ such that an $n$th root of unity has degree at most 2 over $\mathbb{Q}$, following the lead of problem 2. However, I now realize that there is a simpler way, though it puts the use of fields into the background.

Since $\lambda^n = 1$, $\lambda$ lies on the unit circle. If real, $\lambda = 1$ or $-1$ and $n = 1$ or 2. Suppose that $\lambda$ is complex. The other root of the (real) characteristic polynomial will be $\overline{\lambda}$, and $s = \lambda + \overline{\lambda}$. Since $|\lambda| = 1$, $s$ is an integer in the range $-2 < s < 2$. It can only be 1, $-1$, or 0. This leaves us with just six characteristic polynomials to inspect: $x^2 \pm 1$ and $x^2 \pm x \pm 1$. The roots of $x^2 \pm x - 1$ aren’t roots of unity.

It isn’t difficult to find integer matrices $A$ with $A^n = I$, and $n = 1, 2, 3, 4$, or 6. For example, the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & \pm 1 \end{pmatrix}$$

have orders 3 and 6.