Homework 12 Solutions

1 (a) Let F be a field such that $[F : \mathbb{Q}] = 2$. Then F has a basis of two elements over $\mathbb{Q}$. We choose one to be 1 and the other to be x. Thus, $x^2 = (-b)x + (-c)1$, becuase it must be in F and everything in F is a linear combination of $1, x$. Thus, x satisfies $x^2 + bx + c = 0$. So, in particular, $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. Now, $F = \mathbb{Q}(x)$, and so $F = \mathbb{Q}(\frac{-b\pm\sqrt{b^2-4c}}{2})$. However, multplication and addition of rational numbers on x doesn't change $\mathbb{Q}(x)$, and so $F = \mathbb{Q}(\sqrt{b^2 - 4c})$ If b^2-4c has any square factors, we can pull them out, and otherwise clear denominators, so that $F = \mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z}$ which is square free.

(b) If $d_1 = d_2$, then $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$. Now assume that $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ for two square-free integers. Then $\sqrt{d_1} = a+b\sqrt{d_2}$. Squaring both sides, we obtain $d_1 = a^2 + b^2 d_2 + 2ab\sqrt{d_2}$. Now, as a, b, d_1 are rational and $\sqrt{d_2}$ is not, then either $a = 0$ or $b = 0$. If $b = 0$, then $\sqrt{d_1} = a \in \mathbb{Q}$, which is false. Thus, $a = 0$. Then $\sqrt{d_1} = b\sqrt{d_2}$. And so $d_1 = b^2 d_2$. Set $b = \frac{m}{n}$ in lowest terms. Then we have $n^2 d_1 = m^2 d_2$, which contradicts d_1, d_2 being square-free. Thus, $d_1 = d_2$.

(c) The analogue isn't true because the cubic formula requires taking not only cube roots but cube roots of square roots. The analogue of part b is also false, because $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$, as $\sqrt[3]{2}^2 = \sqrt[3]{4}$ and $\sqrt[3]{4}^2 = \sqrt[3]{16} = 2\sqrt[3]{2}$.

2 (a) First off, it is a subgroup. Let $x, y \in \mu_{K,n}$. Then $x^n = y^n = 1$. Look at xy^{-1}. Raise this to the nth power, and we get $(xy^{-1})^n = x^n(y^{-1})^n = x^n y^{-n} = x^n(y^n)^{-1} = 1$. Now all we must show is that the group is cyclic. It is enough to show this for the splitting field of $x^n - 1$ over K, because the nth roots of unity in K will be a subgroup of the nth roots of unity over the splitting field, and so if the group is cyclic over the splitting field, the group must always be cyclic, as it will be a subgroup of a cyclic group. So we must just show that the group is cyclic: let $n = \prod d_i$, with $d_i = p_i^{a_i}$. Now, for each i, we have $x^n - 1 = (x^{d_i} - 1)(x^{n-d_i} + x^{n-2d_i} + \ldots + x^{d_i} + 1)$. So d_i of the nth roots of unity satisfy $x^{d_i} = 1$, but $n - d_i$ don't.

Furthermore, $x^{d_i} - 1 = x^{p_i^{a_i-1}} - 1)(x^{p_i^{a_i} - p_i^{a_i-1}} + \ldots + 1)$. Thus, of the d_ith roots of unity, $p_i^{a_i-1}$ are actually $p_i^{a_i-1}$st roots, but the rest only satisfy $x^{d_i} = 1$. Let u_i be one of these. So u_i has order d_i in the group of d_ith roots of unity. Now, the nth roots of unity form a group of order n, and so it can be written as a direct sum of finite groups of orders d_i. As each of these groups is cyclic by the above argument, their product group is cyclic. Thus, $\mu_{K,n}$ is a cyclic group.

(b) We want to find the group of 12th roots of unity over various fields. For fields containing $\mathbb{Q}$, this is contained in the intersection of the field with the unit circle in the complex plane. Thus, for $\mathbb{Q}, \mathbb{Q}(\sqrt{3}), \mathbb{R}$, the group of twelfth roots of unity is $\{-1, 1\}$. For $\mathbb{Q}(\sqrt{-1})$, the only elements lying on the unit circle are $\{1, -1, i, -i\}$, all of which are twelfth roots of unity. For $\mathbb{Q}(\sqrt{-3})$, we have the sixth roots of unity (see the next problem). For $\mathbb{F}_p$, the multiplicative group is of order $p - 1$. So for $p = 2, 3, 5, 7$, we have $p - 1 = 1, 2, 4, 6$, all of which divide twelve, and so all nonzero elements are 12th roots of unity. For $\mathbb{F}_{11}$, the multiplicative group is of order 10=2*5. So there will only be two twelfth roots, ± 1, which is $\{1, 10\}$.

5 We first make the substitution $y = x^2$. This reduces the equation to $y^2 + y + 1 = 0$, which has solutions $\frac{-1 \pm \sqrt{1-4}}{2} = \omega, \omega^2$. However, this gives $x^2 = \omega, \omega^2$, and so we get $x = \omega, -\omega, \omega + 1, -\omega - 1$. Thus, all four roots are in $\mathbb{Q}(\omega)$, so the splitting field is contained in $\mathbb{Q}(\omega)$. However, $\mathbb{Q}(\omega)$ is the smallest field containing ω, and so must be contained in the splitting field. Thus, $F(\omega)$ is the splitting field.

6 (a) The splitting field of $x^4 + 1$ must contain the solutions to $x^4 + 1 = 0$, that is, $x^4 = -1$. So $x^2 = \pm i$, and $x = \pm\sqrt{\pm i}$. So, we have $\mathbb{Q}(e^{\pi i/4}, e^{-\pi i/4})$. But $e^{-\pi i/4} = e^{7\pi i/4}$, and so the extension is $\mathbb{Q}(e^{\pi i/4})$. Any element of this field can be written as $a + be^{\pi i/4} + ce^{\pi i/2} + de^{3\pi i/4}$, and so the extension has degree 4.

(b) Similarly, we want the smallest field with the solutions to $x^6 + 1 = 0$. The sixth roots of -1. This is the field extension generated by $e^{\pi i/6}$, and so, as above, we find that the degree of the extension is 6.

(c) Things are more complicated for $x^4 - 2 = 0$. This is $x^4 = 2$. So we have $x^2 = \pm\sqrt{2}$, so $x = \sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. To write every element of this field we need 1, $\sqrt[4]{2}$, $\sqrt[4]{4}$, $\sqrt[4]{8}, i\sqrt[4]{2}, i\sqrt[4]{4}, i\sqrt[4]{8}, i$, and so the degree is 8.

(d) For $x^5 - 1 = 0$, we have solution $1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}$ and $e^{8\pi i/5}$. However, the sum of these is zero, and so we only need the first four to write out every element of the field. Thus, this extension has degree 4.

(e) Here we proceed similarly to in problem 5. We make the substitution $y = x^3$, giving us the equation $y^2 + y + 1 = 0$. From above, we know that the solutions are $y = e^{2\pi i/3}$ and $e^{4\pi i/3}$. But $y = x^3$, so we need to take cube roots. We then get $e^{2\pi i/9}, e^{8\pi i/9}, e^{14\pi i/9}, e^{4\pi i/9}, e^{10\pi i/9}, e^{16\pi i/9}$. The field extension is $\mathbb{Q}(e^{2\pi i/9})$, and it is the splitting field of $x^9 - 1$

as well. This, however, gives us a linear relation, and we can express $e^{16\pi i/9}$ as the sum of the others. Thus, we have a splitting field of degree 8.

9 To show that a pentagon is constructible, we can show that the vertices are constructible. The vertices are the fifth roots of unity, that is, the solutions to $x^5 - 1$. Now, 1 is certainly constructible, and so we divide by $x - 1$ to obtain $1 + x + x^2 + x^3 + x^4 = 0$. Because $x \neq 0$, we divide by x^2, and obtain $x^{-2} + x^{-1} + 1 + x + x^2 = 0$. Set $\mu = x + x^{-1}$. Then $\mu^2 = x^{-2} + x^2 + 2$, and so our equation becomes $\mu^2 + \mu - 1 = 0$. So μ satisfies a degree 2 equation over $\mathbb{Q}$, and so is constructible. Now, we have $\mu = x + x^{-1}$. Multiplying through by x, we have $\mu x = x^2 + 1$, so $x^2 - \mu x + 1 = 0$, and so x satisfies a quadratic over $\mathbb{Q}(\mu)$, and so is constructible. Thus, the fifth roots of unity are constructible, and so the pentagon is.