# Problem Set 1 (Solutions)

1. Note $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, as $\sqrt{2}$ is a root of $x^2 - 2$, which is irreducible by Eisenstein's criterion. We will show that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Since $\sqrt{3}$ is a root of $x^2 - 3$, the only way for this to be false is if $x^2 - 3$ splits into linear factors in $\mathbb{Q}(\sqrt{2})$, which would mean $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. If this were true, then $\sqrt{3} = a + b\sqrt{2}$ for some $a, b, \in \mathbb{Q}$. Squaring, we have $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, a contradiction since the left side is rational and the right side is not (if $a$ and $b$ are not equal to 0, but $a = b = 0$ clearly doesn't work). So $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, and by the tower theorem, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

2. Note that $\omega$ is a root of $x^{12} - 1 = 0$. Factoring $x^{12} - 1$, we quickly see that $\omega$ is a root of $x^4 - x^2 + 1$. This is because

$$x^{12} - 1 = (x-1)(x+1)(x^2+1)(x^2+x+1)(x^2-x+1)(x^4-x^2+1),$$

and the the roots of the first three factors are just the fourth roots of unity, the fourth factor has the primitive third roots of unity as roots (as $x^3 - 1 = (x-1)(x^2+x+1)$), and the fifth factor has the negatives of the primitive third roots of unity, which are primitive sixth roots of unity, as roots. So the primitive 12th roots of unity must be roots of the last factor. It suffices to prove that this is irreducible, for then it will be the minimal polynomial over $\mathbb{Q}$ for $\omega$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. Since its roots are the primitive 12th roots of unity, they are all complex, so if it were to factor, it must factor as the product of two quadratics. Write

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 - x^2 + 1.$$

Then $bd = 1$, $bc + ad = 0$, $ac + b + d = -1$, and $a + c = 0$. Subsituting $-a = c$, we have $-a^2 + b + d = -1$ and $a(d - b) = 0$. Then either $a$ is zero or $d = b$.

If $a = 0$, $c = 0$, and we have the equations $bd = 1$ and $b + d = -1$. Adding these gives $bd + b + d = 0$, which factors as $(b+1)(d+1) = 1$, and $b = (1/(d+1)) - 1$. Then $(d/(d+1)) + d = 0$, so $d + d^2 + d = d + 1$, so $d^2 + d - 1 = 0$, and applying the quadratic formula shows that $d$ must be irrational, a contradiction.

If $d = b$, then $b^2 = 1$ so $b = \pm -1$. Then $a^2 = 3$ or $a^2 = -1$, and we get a contradiction, because in each case $a$ is not a rational number.

3. Since $[E_i : F]$ is finite, $E_j = F(S)$ for some finite set $S$. If this were not true, we could find infinitely many elements $s_i \in E_j$ such that $F(\cup_1^{n+1} s_i) \subsetneq F(\cup_1^n s_i)$, which means that each time we add an $s_i$ the degree of the new field over $F$ is strictly larger than the old one. This means we can make the degree arbitrary large, a contradiction.

So $E_1 = F(S_1)$, $E_2 = F(S_2)$, where the $S_i$ are finite sets and we eliminate redundant elements in the $S_j$ so that we have $F(\cup_1^{n+1} s_i) \subsetneq F(\cup_1^n s_i)$ for $s_i \in S_1$ and similarly for $S_2$. Then $[E : F] = [E : E_1][E_1 : F]$, and we get the desired inequality since $[E : E_1] \leq [E_2 : F]$. To see this, call the elements of $S_2$ as $t_i$ and note that $[E_2 : F] = [F(t_1) : F][F(t_1, t_2) : F(t_1)] \cdots [F(S) : F(S - t_k)]$. Similarly, as $E = F(S_1 \cup S_2)$ and $E_1 = F(S_1)$, we have $[E : E_1] = [E_1(t_1) : E_1] \cdots [E : E_1 - t_k]$. We have $[F(t_1) : F] \geq [E_1(t_1) : E_1]$, as $E_1 \subset F$, so the minimal polynomal for $t_1$ over $F$ is also a polynomial over $E_1$. So the minimal polynomial for $t_1$ over $E_1$ divides the minimal polynomial for $t_1$ over $F$, and hence has degree less than or equal to it, giving $[F(t_1) : F] \geq [E_1(t_1) : E_1]$. Repeating this for each term in the factorization shows $[E : E_1] \leq [E_2 : F]$ and implies the desired inequality.

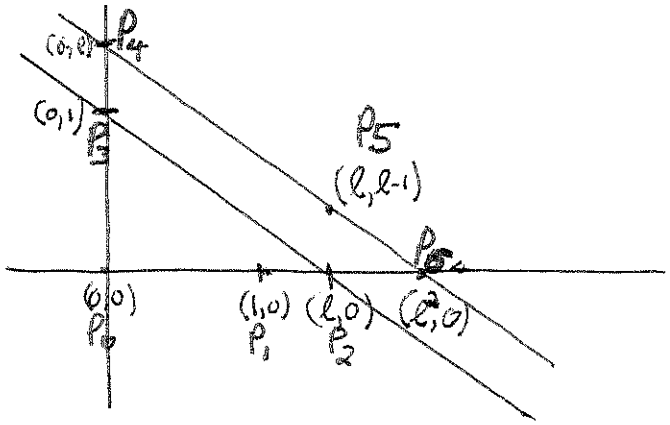
(4) Let $E = F(u)$, $u$ transcendental, and let $K \neq F$ be a subfield of $E/F$. Show that $u$ is algebraic over $K$.

Choose some $x \in K \backslash F$, then $x = f(u)/g(u)$ with $f, g \in F[x], g \neq 0$ and at least one of them has positive degree. Let us denote $f(u) = \sum a_i u^i, g(u) = \sum b_j u^j$ and since $f(u) = xg(u)$, by letting $c_i = a_i - xb_i$, we have $\sum c_i u^i = 0$, which shows $u$ is algebraic over $K$. □

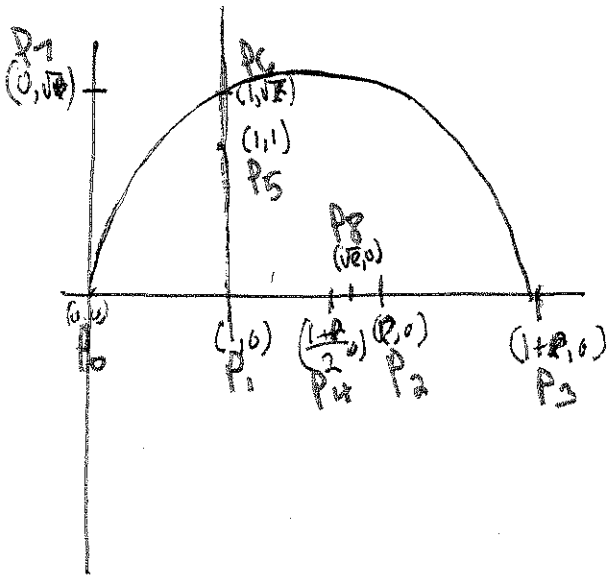
(5) Given that $(\ell, 0)$ is constructible ($\ell \in \mathbb{R}_+$), show how to construct $(\sqrt{\ell}, 0)$ and $(\ell^2, 0)$

5/5

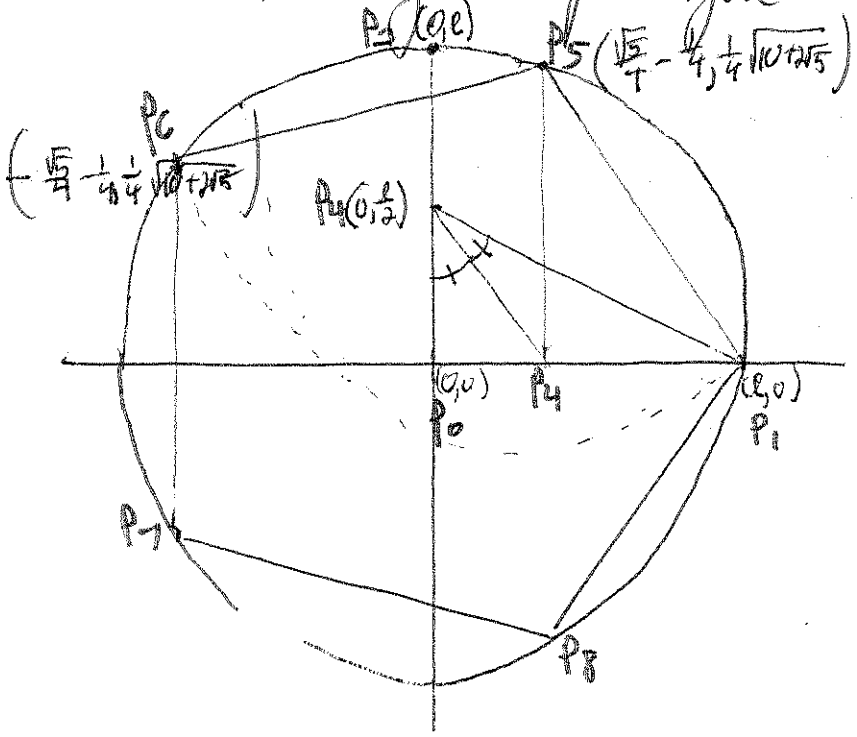
$(\ell^2, 0)$




$(\sqrt{\ell}, 0)$



(6) Construct a regular pentagon.




5/5

(7) Construct a splitting field over $\mathbb{Q}$ of $x^5-2$. Find its dimensionality over $\mathbb{Q}$.

Let $\xi$ be the primitive 5-th root of unity in $\mathbb{C}$ and let $\alpha=\sqrt[5]{2}$. $x^5-2$ has roots $\alpha,\alpha\xi,\alpha\xi^2,\alpha\xi^3,\alpha\xi^4$ in $\mathbb{C}$, hence the splitting field of $x^5-2$ is $L:=\mathbb{Q}(\alpha,\xi)$.

To determine the dimensionality, first note $[\mathbb{Q}(\alpha):\mathbb{Q}]=5$ since $\alpha^5-2$ is irreducible and $[\mathbb{Q}(\xi):\mathbb{Q}]=4$ for that the cyclotomic polynomial $\Phi_5$ is the minimal polynomial of $\xi$ and hence $[L:\mathbb{Q}]$ should be divisible by $4\cdot 5=20$. Now since $\alpha$ is a root of $x^5-2\in\mathbb{Q}(\xi)[x]$ and $\deg(x^5-2)=5$, we must have $[L=\mathbb{Q}(\xi))(\alpha):\mathbb{Q}(\xi)]\leq 5$. Therefore

$$[L:\mathbb{Q}]=[L:\mathbb{Q}(\xi)][\mathbb{Q}(\xi):\mathbb{Q}]\leq 20.$$

However we've shown $[L:\mathbb{Q}]$ is divisible by 20 and it follows that $[L:\mathbb{Q}]=20$.

(8) Determine a splitting field over $\mathbb{Z}/(p)$ of $x^{p^e}-1$, $e\in\mathbb{N}$.

Since $x^{p^e}-1=(x-1)^{p^e}$ in $\mathbb{Z}_p$ (note $1=-1$ in $\mathbb{Z}_2$), the splitting field of $x^{p^e}-1$ is $\mathbb{Z}_p$ itself. □

(9) Find splitting field extensions for $x^3-5$ over $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$.

(a) Note $x^3-1$ splits in $\mathbb{Z}_7$ as $x^3-1=(x-1)(x-2)(x-4)$, so the splitting field would be $\mathbb{Z}_7(\sqrt[3]{5})$.

(b) $x^3-5$ has one root $x=3\in\mathbb{Z}_{11}$ and $x^3-5=(x-3)(x^2+3x-2)$. The roots of $x^2+3x-2$ in $\mathbb{C}$ are $\frac{-3\pm\sqrt{17}}{2}$ and consider the field $\mathbb{Z}_{11}(\sqrt{6})$, in which $x^3-5$ factors as $x^3-5=(x-3)(x-(4+6\sqrt{6}))(x-(4-6\sqrt{6}))$ and hence it is the desired splitting field.

(c) $x^3-5=(x-7)(x-8)(x-11)$ in $\mathbb{Z}_{13}$ and therefore the desired splitting field is itself. □

(10) Suppose that $M/L$ and $L/K$ are extensions, and that $\alpha\in M$ is algebraic over $K$. Does $[L(\alpha):L]$ always divide $[K(\alpha):K]$?

No. Let $K=\mathbb{Q},L=\mathbb{Q}(\sqrt[3]{2}),M=\mathbb{C}$ and let $\alpha=\sqrt[3]{2}\exp(2\pi i/3)$. Then $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ and since $\alpha\notin L$ and $\alpha^2/(\sqrt[3]{2})^2+\alpha/\sqrt[3]{2}-1=0$, $[L(\alpha):L]=2$.

15