Exersise 6.1

For $n = p_1^{a_1} \dots p_r^{a_r}$ being the prime factorization of n we have the equality

$$\prod_{i=1}^{r} \mathbb{Q}(\zeta_{p_i^{a_i}}) = \mathbb{Q}(\zeta_n)$$

We have '$\subseteq$' by the fact that $\mathbb{Q}(\zeta_n)$ contains each $\mathbb{Q}(\zeta_{p_i^{a_i}})$ (since $\zeta_n^{n/p_i^{a_i}}$ is a primitive $p_i^{a_i}$ root of unity, $\zeta_n | \zeta_{p_i^{a_i}}$) and thus must contain the composite. We have '$\supseteq$' by the fact that the product

$$\zeta = \zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \dots \zeta_{p_r^{a_r}}$$

is a primitive nth root of unity.
We can use a simple inductive argument on r to show

$$\cap_{i=1}^{r} \mathbb{Q}(\zeta_{p_i^{a_i}}) = \mathbb{Q}$$

as well as

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \times_{i=1}^{r} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q})$$

For the base case $r = 2$, using the identity for Galois Extensions $K_1/\mathbb{Q}, K_2/\mathbb{Q}$

$$[K_1K_2 : \mathbb{Q}] = \frac{[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]}$$

Where $K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}}), K_2 = \mathbb{Q}(\zeta_{p_2^{a_2}}),\ K_1K_2 = \mathbb{Q}(\zeta_n)$. Since

$$[K_1K_2 : \mathbb{Q}] = \varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$$

we have $[K_1 \cap K_2 : \mathbb{Q}] = 1 \Rightarrow K_1 \cap K_2 = \mathbb{Q}$. From the problem 3 statement from last week we get the other statement

$$\mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$$

For the inductive step we let $K_1 = \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p_i^{a_i}})$ and $K_2 = \mathbb{Q}(\zeta_{p_{r+1}^{a_{r+1}}})$ and once again we have

$$[K_1K_2 : \mathbb{Q}] = \varphi(n) = \varphi(p_1^{a_1}) \dots \varphi(p_r^{a_r})\varphi(p_{r+1}^{a_{r+1}}) = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$$

so $[K_1 \cap K_2 : \mathbb{Q}] = 1 \Rightarrow K_1 \cap K_2 = \mathbb{Q}$. Thus from the inductive hypothesis

$$\cap_{i=1}^{r} \mathbb{Q}(\zeta_{p_i^{a_i}}) \cap \mathbb{Q}(\zeta_{p_{r+1}^{a_{r+1}}}) = \mathbb{Q}$$

$$\cap_{i=1}^{r+1} \mathbb{Q}(\zeta_{p_i^{a_i}}) = \mathbb{Q}$$

We also have

$$\mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q})$$

which by the inductive hypothesis

$$\cong \times_{i=1}^{r} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_{r+1}^{a_{r+1}}})/\mathbb{Q}) \cong \times_{i=1}^{r+1} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q})$$

Exersise 6.2

By the classification of finite abelian groups we know

$$G = \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_r)$$

where $n_1|n_2|\dots|n_r$. We can choose primes $p_1, p_2 \dots p_r$ so that $p_i \equiv 1 \mod n_i$. Letting $n = p_1 \dots p_r$ we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_r})/\mathbb{Q})$$

$$= \mathbb{Z}/(\varphi(p_1)) \times \mathbb{Z}/(\varphi(p_2)) \times \cdots \times \mathbb{Z}/(\varphi(p_r))$$

Since p_i is prime $\varphi(p_i) = p - 1$ and thus since $p_i \equiv 1 \mod n_i, n_i|p_i - 1$, there is a subgroup of order n_i, $\mathbb{Z}/(n_i) \subset \mathbb{Z}/(p_i - 1)$. Thus

$$G = \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_r) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

Thus from the fundamental theorem of Galois theory there exists a subfield $K \subset \mathbb{Q}(\zeta_n)$ such that

$$\mathrm{Gal}(K/\mathbb{Q}) \cong G$$

Exersise 6.3

It is a well known result the center of the n-gon can be constructed by the intersection of two lines of opposing corners for the n even case and the intersection of two lines each through some corner and perpendicular to the opposing side for the n odd case. Thus we can assume without loss of generality the n gon is centered at the origin

We have that the points on the regular n-gon centered at the origin coincides with the position of the nth roots of unity when viewed geometrically as elements of $\mathbb{R}^2$. Thus the n-gon is constructable if and only if $\zeta_n = (\cos(2\pi/n), \sin(2\pi/n)) \in \mathbb{R}^2$ is constructable.

We know that a length $d \in \mathbb{R}$ is constructable if and only if

$$[\mathbb{Q}(d) : \mathbb{Q}] = 2^k$$

for some k

Thus ζ_n is constructable if and only if both $\alpha = \cos(2\pi/n)$ and $\beta = \sin(2\pi/n)$ are constructable as lengths. Since $\alpha = \frac{\zeta_n + \zeta_n^{-1}}{2}$ (where ζ_n is no longer viewed as a geometric object)

$$\mathbb{Q}(\alpha), \mathbb{Q}(i\beta) \subset \mathbb{Q}(\zeta_n)$$

If $\varphi(n) = 2^k$ then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\beta) : \mathbb{Q}]$ divide $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, and so both α and β are even power degree extensions of $\mathbb{Q}$ and thus constructable. Thus the n-gon is constructable

Conversly if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = 2^k m$ for some odd $m > 1$ then since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \mathbb{Z}/(2^k m)$ there is a subgroup of order 2^k with corresponding fixed field F where $[F : \mathbb{Q}] = m$. Since

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha)\mathbb{Q}(i\beta)$$

it must be the case that F intersects $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\beta)$ nontrivially (the intersection must be a field strictly larger than $\mathbb{Q}$). The intersection must have odd degree over $\mathbb{Q}$ since it must divide the degree of F and thus either $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ or $[\mathbb{Q}(\beta) : \mathbb{Q}]$ has an odd factor, which means they are not constructable. Thus the n-gon is not constructable.

To describe the n such that $\varphi(n) = 2^k$, letting $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ be the prime factorization we have

$$\varphi(n) = \prod \left(p_i^{a_i} - p_i^{a_i - 1}\right)$$

Since the only possible divisors of 2^k are powers of 2, it must be the case $p_i^{a_i} - p_i^{a_i-1} = p^{a_i-1}(p_i - 1) = 2^{s_i}$ for some s_i. Thus either $p_i = 3, a_i = 1$ or $p_i = 2$. Thus n is of the form $2^k \cdot 3$ or 2^k

Exersise 6.4

Letting $f(x) = x^5 + 20x + 16$, we have that the discriminant of f is a square in $\mathbb{Q}$ and thus $\sqrt{D(f)}$ is fixed under all automorphisms

$$D(f) = 2^{16} 5^6$$

(I calculated the discriminant using the discriminant function in sage)

Thus the Galois group G must be contained in A_5

We have

$$f(x-1) = x^5 - 5x^4 + 10x^3 - 10x^2 + 25x - 5$$

An application of Eisenstiens criteria with $p = 5$ shows that $f(x-1)$ and thus f are irredicible. Thus Letting K be the splitting field of f, we know that $5||\mathrm{Gal}(K/\mathbb{Q})|$.

The only elements of order 5 in S_5 are five cycles, thus there exists a five cycle in $\mathrm{Gal}(K/\mathbb{Q})$ when viewed as a subgroup of S_5

We have that the derivative has no real zeros

$$f' = 5x^4 + 20$$

$$f'(x) = 0 \Rightarrow x^4 = -4$$

Thus f has only one real root. Thus the congugation automorphism of $\mathbb{C}$ must swap two pairs of complex roots of f. This corresponds to a product of two 2-cycles in S_5

It is a well known fact that A_5 is generated by a 5-cycle and any product of two 2-cycles. Thus G must contain A_5.

Exersise 6.5

We have that the primitive 29th root of unity ζ has Galois group

$$G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/(29))^\times$$

The multiplicative group of integers modulo n have been classified up to large orders. In the case of $n = 29$ we have

$$(\mathbb{Z}/(29))^\times \cong \mathbb{Z}/(28) \cong \mathbb{Z}/(4) \times \mathbb{Z}/(7)$$

And 2 is a generator of $(\mathbb{Z}/(29))^\times$
Letting $H = \mathbb{Z}/(4)$ be the subgroup of the galois group, since G is generated by the automorphism

$$\zeta \to \zeta^2$$

we have that H is generated by the 7th power of this automorphism

$$\zeta \to \zeta^{2^7} = \zeta^{12}$$

The fixed field $K = \mathbb{Q}(\zeta)^H \subset \mathbb{Q}(\zeta)$ is a Galois extension (since $\mathbb{Z}/(4)$ is normal) with Galois group

$$\text{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/(28))/(\mathbb{Z}/(4)) \cong \mathbb{Z}/(7)$$

Thus the minimal polynomial of some generator for K is degree 7 with cyclic Galois Group. Since $K \subset \mathbb{Q}(\zeta)$, the trace of ζ over H is a generator

$$\alpha = \text{Tr}_H(\zeta) = \zeta + \zeta^{12} + \zeta^{28} + \zeta^{17}$$

The reason for this is because for any $\sigma \in H$ we know $\alpha^\sigma = \alpha$ and also we know for any $\tau \in G \setminus H$, $\alpha^\tau \neq \alpha$ since if it were the case that $\alpha^\tau = \alpha$ then τ would have to send ζ to the same image of some $\sigma \in H$ which would mean $\tau = \sigma$ which is a contradiction. Thus we have

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha)) = H \Rightarrow \mathbb{Q}(\alpha) = K$$

If we find a polynomial f of degree 7 where $f(\alpha) = 0$ then we are done.
To find this polynomial we can solve the system of equations:

$$a_7\alpha^7 + a_6\alpha^6 + \dots a_1\alpha + a_0 = 0$$

where the coefficeint of each ζ^n must equal 0.
Using Sage I solved this system of equations to yield the polynomial

$$f(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$$

Exersise 6.6

Letting K be the splitting field of f over ℓ. Let $f = f_1 f_2 \dots f_n$ be the prime factorization of f over $\ell[x]$. For any root α of f_1 and root β of f_i, α and β roots of the same seperable irredicible polynomial f over k and thus there exists an isomorphism

$$\varphi : k(\alpha) \to k(\beta)$$

Which extends to an automorphism (since K is a splitting field)

$$\overline{\varphi} : K \to K$$

If we restrict $\overline{\varphi}$ to $\ell(\alpha)$, we have that $\overline{\varphi}(\ell) = \ell$ since ℓ is Galois over k and $\overline{\varphi}(\alpha) = \beta$. Thus $\overline{\varphi}|_{\ell(\alpha)}$ is an isomorphism

$$\overline{\varphi}|_{\ell(\alpha)} : \ell(\alpha) \to \ell(\beta)$$

so

$$\ell[x]/(f_1) \cong \ell[x]/(f_i)$$

so $\deg(f_1) = \deg(f_i)$ for each i