Answers to HW13

197. Over $\mathbb{Z}_p$, the polynomial $x^n - 1$ factors into linear factors (whose roots, therefore, are all $n$th roots of unity in characteristic $p$). Let $n = p^r m$ where $m$ is not divisible by $p$. Then $x^n - 1 = (x^m - 1)^{p^r}$, i.e. all $n$th roots of unity in characteristic $p$ are actually $m$th roots of unity (occurring in $x^n - 1$ with multiplicity $p^r$). Since $p^r$ and $m$ are coprime, $\varphi(n)$ is divisible by $\varphi(m)$, and hence $\mathbb{F}_{p^r(m)} \subset \mathbb{F}_{p\varphi(n)}$. By Euler’s theorem, $p^{\varphi(m)} \equiv 1 \mod m$, and therefore the cyclic group $\mathbb{F}_{p^r(m)}$ of order $p^{\varphi(m)} - 1$ contains all $m$ distinct $m$th roots of unity.

Remark. When $n = m$ is not divisible by $p$, the solution amounts to the last sentence.

198. Over $\mathbb{Z}_p$, we still have $\prod_{d|n} \psi_d(x) = x^n - 1$ which implies that the roots of $\psi_n$ in $\mathbb{Z}_p$ are still the $\varphi(n)$ generators of the cyclic subgroup of $n$th roots of unity in $\mathbb{F}_{p^{\varphi(n)}}^\times$ (according to the previous exercise in the case when $n$ is not divisible by $p$).

Let $\zeta$ be one of such generators, and suppose that $\psi_n$ factors over $\mathbb{Z}_p$ non-trivially as $fg$, where $f(\zeta) = 0$. Then $f(\zeta^p) = 0$.

The argument could be the same as in the proof of irreducibility of $\psi_n$ in $\mathbb{Z}[x]$. Namely, if $g(\zeta^p) = 0$, then $\zeta$ is a root of $g(x^p) = (g(x))^p$, i.e. $g(\zeta) = 0$. This implies that $f$ and $g$ are not coprime in $\mathbb{Z}_p[x]$ and contradicts the simplicity of the roots of $\psi_n$ (and of $x^n - 1$).

Alternatively, $f(\zeta^p) = 0$ since $\zeta^p = \Phi(\zeta)$ is obtained from $\zeta$ by the Frobenius automorphism of $f$.

Consequently $\zeta, \Phi(\zeta), \Phi^2(\zeta), \ldots$ all are roots of $f$. Let $k > 0$ be the smallest such that $\Phi^k(\zeta) = \zeta$. Then $k \leq \deg f < \deg \psi_n = \varphi(n)$. But $\zeta^{p^k} = \zeta$ means that $p^k \equiv 1 \mod n$ (since $\zeta$ is a generator of the cyclic group of $n$th roots of unity). Therefore reducibility of $\psi_n$ over $\mathbb{Z}_p$ implies that the order of $p$ in $\mathbb{Z}_p^\times$ is smaller than $\varphi(n)$.

Conversely, let $p^k \equiv 1 \mod n$ for some positive $k < \varphi(n)$. We have: $\zeta^{p^k} = \zeta$. Then the polynomial $F(x) := \prod_{i=1}^k (x - \Phi^i(\zeta))$ is invariant under $\Phi$, and therefore has coefficients in $\mathbb{Z}_p$. Thus $f$ is a non-trivial divisor of $\psi_n$ in $\mathbb{Z}_p[x]$.

Remark. The alternative, i.e. the irreducibility of $\psi_n$ over $\mathbb{Z}_p$, is equivalent to $p$ being a generator of $\mathbb{Z}_p^\times$, and in particular requires that the multiplicative group $\mathbb{Z}_p^\times$ is cyclic. It is a separate problem to find out for which $n$ it is cyclic. It is not very hard to show that this happens if and only if $n$ is any power $q^r$ of an odd prime $q$, or $n = 2$ or $4$. Thus, in all other cases $\psi_n$ is reducible over $\mathbb{Z}_p$ (where $p \nmid n$).
202. Since 3 is a generator of $\mathbb{Z}_{17}^*$, the automorphism $\sigma : \zeta \mapsto \zeta^3$ of the cyclotomic field $\mathbb{Q}(e^{2\pi i/17})$ and its powers map $\mu_1 = \zeta + \zeta^{-1}$ into all other $\mu_j = \zeta^j + \zeta^{-j}$, $j = 2, \ldots, 8$. Therefore the subfield $\mathbb{Q}(\mu_1)$ has degree 8 over $\mathbb{Q}$ and thus must coincide with the subfield fixed by $\sigma^8$.

Remark. Complex conjugation induces an order 2 automorphism of the cyclotomic field, and hence must coincide with $\sigma^8$.

203. Let $\zeta := e^{2\pi i/5}$. The Galois group $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{Z}_5^*$ is generated by $\sigma : \zeta \mapsto \zeta^2$. So, the sequence $\{\sigma^k(\zeta)\}$ is $\zeta, \zeta^2, \zeta^{-1}, \zeta^{-2}$. The Gauss sums generating the quadratic extension intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ are $\eta_+ := \zeta + \zeta^{-1} = 2\cos 2\pi/5$ and $\eta_- := \zeta^2 + \zeta^{-2} = 2\cos 4\pi/5$. They are roots of $x^2 + x - 1$ since $\eta_+ + \eta_- = -1 = \eta_+\eta_- = \zeta^3 + \zeta^{-3} + \zeta^1 + \zeta^{-1}$. Thus, $2\cos 2\pi/5 = (\sqrt{5} - 1)/2$ is the famous golden ratio, and can be easily constructed by straightedge and compass.