

Dummit & Foote (3.2) 16, 18, 19, 22

3.2.16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

3.2.18 Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

3.2.19 Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

3.2.22 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n , where φ denotes Euler's φ -function.