(1) If G is a finite simple group of order n, find the # of normal subgroups of $G\times G$.

Solution/ A subgroup of $G\times G$ looks like $H\times K$, and if $H\times K \trianglelefteq G\times G$, then $H, K \trianglelefteq G$.

Thus there are 4 normal subgroups: $\{1\}\times\{1\}$, $\{1\}\times G$, $G\times\{1\}$, $G\times G$.

(2) (a) State Feit-Thompson: If G is a finite group of odd order, it is solvable.

(b) W/O using Feit-Thompson, show that $\nexists$ simple group of order 6545: $5\cdot 7\cdot 11\cdot 17$

• Let $|G|=6545$.

$n_5=11$. $\quad n_7 \mid 6545$ and $n_7\equiv 1 \bmod 7$, so $n_7=85$

$n_{11}=595$

$n_{17}=35$

Since any two Sylow p-subgroups intersect trivially for $p\in\{5,7,11,17\}$,

G has $11\cdot 4$ els of order 5 : 44

$85\cdot 6$ els of order 7 : 510

$595\cdot 10$ .. .. 11 : 5950

$35\cdot 16$ .. .. 17 : 560

so by counting elements....

(3) (a) R a ring, $I\subseteq J$ ideals. Prove $(R/I)/(J/I)\cong R/J$.

(b) Example of a UFD that is not a PID. Prove it is not a PID.

(c) Let R be a PID. If $a,b,c\in R$ are s.t. $\gcd(a,b)=1=\gcd(a,c)$. Show $\gcd(a,bc)=1$

Proof/ (a) Consider the map $\varphi: R/I\to R/J$ sending $(a+I)\mapsto(a+J)$

Then $\ker\varphi = J/I$ and this is an isomorphism as

$(a+I)+(b+I)=(a+b)+I \xmapsto{\varphi} (a+b)+J$

$\varphi(a+I)+\varphi(b+I)=(a+b)+J$

and $(a+I)(b+I)=ab+I \xmapsto{\varphi} ab+J$

$\varphi(a+I)\varphi(b+I)=ab+J$

(b) $\mathbb{Z}[x,y]$ is a UFD but not a PID as (x,y) is not principal

(c) Need to show if $d\mid a$ and $d\mid bc$, then $d=1$.

$R=(a,b)=(d)$, $d=1$ and $(a,c)=(d)=R$

so $\exists\ x,y$ s.t. $ax+by=1$,

u,v s.t. $au+cv=1$

Then $bcyv=(1-ax)(1-au)$

$=1-a(x+u)+a^2xu$

$a(x+u-axu)+(bc)yv=1$

so $(a,bc)=R$ and thus $\gcd(a,bc)=1$.

(4) F a field, V,W fin. dim. vector spaces over F, and $T:V\to W$ a linear transformation.

(a) Let $\{w_1,\dots,w_r\}$ be a basis for $T(V)$, and $\{v_1,\dots,v_r\}\subseteq V$ s.t. $T(v_j)=w_j$.

Prove $v_1,\dots,v_r$ are linearly independent. Let $U=\operatorname{span}\{v_1,\dots,v_r\}$, $K=\ker T$.

Prove the theorem $\operatorname{rank}(T)+\operatorname{nullity}(T)=\dim(V)$ by showing $V=U\oplus K$.

(b) Show any linearly independent set $\{v_1,\dots,v_m\}\subseteq V$ extends to a basis.

Proof/ (a) If $v_1,\dots,v_r$ not L.I., $c_1v_1+\dots+c_rv_r=0$,

$T(\quad\uparrow\quad)=0$

$c_1w_1+\dots+c_rw_r=0$, not a basis.

If $T(v_i)=0$ then $v_i=0$, or $v_i\notin\operatorname{span}\{v_1,\dots,v_r\}$

thus $v_i\in K$.

Extending $v_1,\dots,v_r$ to a basis $v_1,\dots,v_n$ (see proof of exchange lemma).

we have $\{v_{r+1},\dots,v_n\}$ span $\ker T$, so $V=U\oplus K$,

and as $\dim U=\operatorname{rank} T$, this shows rank-nullity theorem.

(b) Proof of exchange lemma.

(Proof of exchange lemma)

Let $\{b_1,\dots,b_m\}$ be L.I. and $\{a_1,\dots,a_n\}$ a basis. Then $\forall\, k\le m$ $\exists$ ordering of a's.

$\{b_1,\dots,b_k,a_{k+1},\dots,a_n\}$ is a basis.

Induct on k. If $k=0$, nothing to be done. Else let $\{b_1,\dots,b_k,a_{k+1},\dots,a_n\}$ be a basis. Then

$b_{k+1}=\beta_1b_1+\dots+\beta_kb_k+\alpha_{k+1}a_{k+1}+\dots+\alpha_na_n$

We may assume $\alpha_{k+1}\neq 0$ as if all $\alpha_i=0$, the b_i's would be L.D.

Then we may solve for a_{k+1} to show

$\{b_1,\dots,b_k,b_{k+1},a_{k+2},\dots,a_n\}$ is still a spanning set.

If $\beta_1b_1+\dots+\beta_{k+1}b_{k+1}+\alpha_{k+2}a_{k+2}+\dots+\alpha_na_n=0$

then replace b_{k+1} to show contradiction of inductive hypothesis.

(5) Suppose $K[\alpha]/K$ is an extension, that α is algebraic over K but not in K, and β is transcendental over K.

Prove $K(\alpha, \beta)$ is not a simple extension.

<u>Proof</u>: Suppose that $K(\alpha, \beta) = K(\gamma)$.

Then, $\alpha = c\gamma + d$ for $c, d \in K$

and as α is algebraic over K,

$$a_n\alpha^n + \dots + a_1\alpha + a_0 = a_n(c\gamma+d)^n + \dots + a_1(c\gamma+d) + a_0 = 0$$

and thus γ is algebraic over K.

But, $\beta = c'\gamma + d'$ and as

$$b_n\gamma^n + \dots + b_1\gamma + b_0 = 0,$$

$\gamma = \frac{\beta - d'}{c'}$, we can multiply by $(c')^n$ to clear denoms & show β is algebraic over K. ∎

(6) Let $h(x) = x^4 + 1$.
(a) Show $\pm\frac{\sqrt{2}}{2}(1 \pm i)$ are the roots of h in $\mathbb{C}$.
(b) Find $a \in \mathbb{C}$ s.t. $L = \mathbb{Q}(a)$ is the splitting field of h in $\mathbb{C}$.
(c) Describe $Gal(L/\mathbb{Q})$ as a group of permutations of roots of $h(x)$, and as a group of automorphisms of L.
(d) Find all intermediate fields $\mathbb{Q} \subseteq M \subseteq L$, and for each find the subgroup of $G = Gal(L/\mathbb{Q})$ fixing it. Which of these extensions are normal?

$$h\left(\pm\frac{\sqrt{2}}{2}(1 \pm i)\right) = \frac{1}{4}(1+i)^4 + 1 = \frac{1}{4}(1 + 4i - 6 - 4i + 1) + 1 = 0$$

$$= \frac{1}{4}(1-i)^4 + 1 = \frac{1}{4}(1 - 4i - 6 + 4i + 1) + 1 = 0.$$

(b) If ζ is a primitive 8^{th} root of unity,

$\{\zeta, \zeta^3, \zeta^5, \zeta^7\} = \{\pm\frac{\sqrt{2}}{2}(1 \pm i)\}$ comes from $\left(e^{2\pi i k/8}\right)$

so $L = \mathbb{Q}(\zeta)$ is the splitting field of h.

(c) An automorphism of $L/\mathbb{Q}$ sends ζ to ζ^k, $k \nmid 8$.