

Chris Crossade

A

~~39/40~~

39/40

① find the # of elems of order 11 in  
a simple group of order  $2^2 \cdot 11 \cdot 17$

9/10 We know the number of 11-sylow subgroups  
is  $1 \pmod{11}$  and divides  $2^2 \cdot 11 \cdot 17$ ,  
and each element of order 11 lives in  
a (unique!) such subgroup. ~~OK~~

(since any two cyclic groups of prime order  $\neq 1$   
intersect nontrivially, they are the same exactly 11  
order is exactly 11 (it is below))

Now the only valid choices are 1 or 34 subgroups, but it cannot be  
1, as  $G$  is simple (so the 11-sylow subgroup  
is not normal)

So there are 34 11-sylow subgroups,  
each contributing exactly 10 elements  
of order 11. This gives 340 total.  
No repetitions ✓ ~~OK~~

(2) Let  $P$  be a  $p$ -Sylow subgroup of  $G$ .

$H \leq N_G P$  a  $p$ -group. Show  $H \subseteq P$ .

Since  $P \leq N_G P$ , we know  $P$  is the unique  $p$ -Sylow subgroup of  $N_G P$ . ✓

As  $H$  is a  $p$ -group contained in  $N_G P$ , it must be contained in some Sylow  $p$ -group, but the only choice is  $P$ .

So  $H \leq P$ , as desired. ✓

~~3~~ Chris Crossaek

[A]

③ let  $G$  be a simple group of even order. Show  $G$  is generated by elements of order 2.

let  $H = \langle x_i \mid x_i^2 = 1 \rangle \leq G.$

since  $|G|$  is even, it has an element of order 2, so  $H \neq 1.$

Now, note  $H \trianglelefteq G$ , since each generator conjugates to another generator:

for any  $g, x^2 = 1$ :

$$(g^{-1} x g)^2 = g^{-1} x^2 g = g^{-1} g = 1$$

So  $H \neq 1$  is normal in  $G$ , so by simplicity  $H = G.$

④ let  $Z$  be the center of  $G$ .

10/10 if  $G/Z$  is cyclic, then  $G$  is abelian.

Let  $x, y \in G$ . Say  $G/Z$  is generated by  $gZ$ .

then  $xZ = (gZ)^k = g^k Z$ ,  $yZ = (gZ)^l = g^l Z$

in  $G/Z$ . So  $x = g^k z_1$ ,  $y = g^l z_2$  (in  $G$ )  
for some  $z_1, z_2 \in Z$ . ✓

$$\text{Now } xy = g^k z_1 g^l z_2 = g^l z_2 g^k z_1 = yx \quad \checkmark$$

since  $z_1, z_2$  commute with everything,

and  $g^k, g^l$  commute with each other. ✓

Chris Grossacke

10, 10, 10, 10, N  $\rightarrow$  40

13

① Show  $M_{n \times n}(\mathbb{Z})$  has a nontrivial  
(2-sided) ideal

Look at  $E \triangleq \{A \in M_{n \times n}(\mathbb{Z})\}$   
the matrices with even entries.

this is clearly closed under +, and  
contains 0.

Moreover, if A is any matrix  
and  $M \in E$ :

$(AM)_{ij} = \sum_k A_{ik} M_{kj}$  is a sum of  
even numbers (since each  $M_{kj}$  is even).

Showing  $(MA)_{ij}$  is even is similar,

and we see  $E$  is a 2-sided ideal,  
(oh, it's nontrivial because it's clearly  
nonzero (put a 2 in one entry) and not  
everything (doesn't contain the identity matrix))

② Let  $R = \mathbb{C}[x]$ ,  $M$  an  $R$ -mod that's a f-dim  $\mathbb{C}$ -VS. Say  $m \in M$  is not an eigenvector for  $x$ . Then  $\text{Hom}_R(M, M) \rightarrow \text{Hom}_{\mathbb{C}}(M, M)$  is not surjective.

Extend  $\{m, xm\}$  to a basis  $\{m, xm, v_1, \dots, v_k\}$  of  $M$  as a  $\mathbb{C}$ -vector space. (note  $m, xm$  are independent since  $m$  is not an eigenvector)

let  $L: M \rightarrow M$  be the map of  $\mathbb{C}$ -VS's

linearly extending

$$\begin{aligned} m &\mapsto m \\ v_i &\mapsto 0 \quad \forall i \\ xm &\mapsto 0 \end{aligned}$$

now  $L \in \text{Hom}_{\mathbb{C}}(M, M)$ , but  $L$  is not the restriction of an  $R$ -linear map, since if it were, we would have:

10

$$0 = L(xm) = xLm = xm \neq 0 \quad \times$$

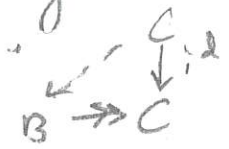
(again, note  $xm \neq 0$  since otherwise  $m$  would be an eigenvector w/ eigenvalue 0)

**13**

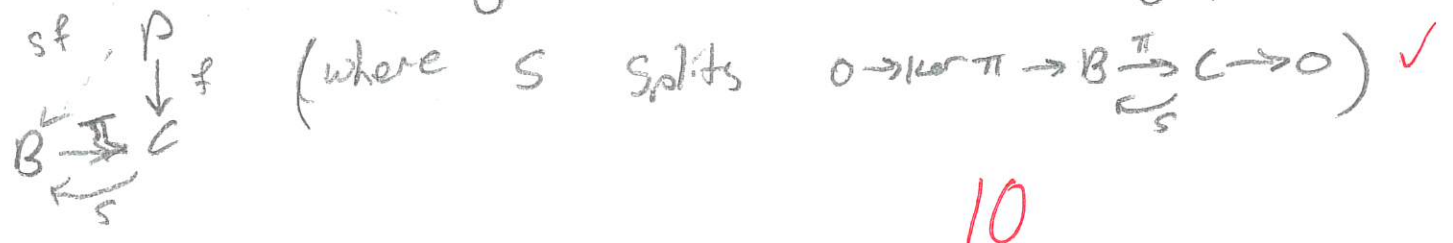
- (3) let  $R$  be a (unital) ring. TFAE
- I** every (unital)  $R$ -mod is projective
  - II** " " " " injective

We show **I**  $\Leftrightarrow$  "every short exact sequence splits"  $\Leftrightarrow$  **II**

if every  $C$  is projective, then every  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  splits by considering



Conversely if every SES splits, then every  $P$  is projective:



10

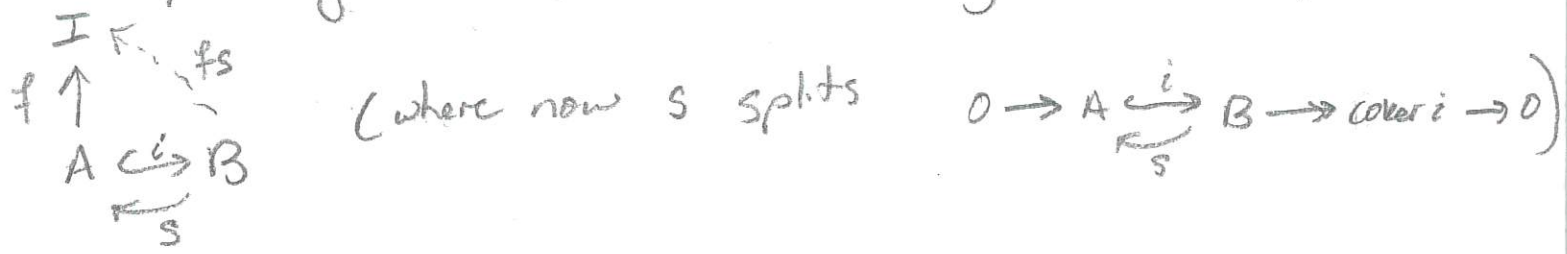
So **I**  $\Leftrightarrow$  "every SES splits",

Dually, if every  $A$  is injective, then every

$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  splits by considering



and if every SES splits then every  $I$  is injective:



So "every SES splits"  $\Leftrightarrow$  **II**, and we're done.

$$\textcircled{4} \text{Hom}_{\mathbb{R}}(M, \text{Hom}_{\mathbb{R}}(N, P)) \cong \text{Hom}_{\mathbb{R}}(N, \text{Hom}_{\mathbb{R}}(M, P)) \dots$$

By yoneda, it suffices to show (naturally in  $X$ )

$$\text{Hom}(X, \text{Hom}_{\mathbb{R}}(M, \text{Hom}_{\mathbb{R}}(N, P))) \cong \text{Hom}(X, \text{Hom}_{\mathbb{R}}(N, \text{Hom}_{\mathbb{R}}(M, P)))$$

but by the tensor hom adjunction and commutativity of  $\otimes$ , we have:

$$\begin{aligned} \text{Hom}(X, \text{Hom}_{\mathbb{R}}(M, \text{Hom}_{\mathbb{R}}(N, P))) &\cong \text{Hom}(X \otimes M, \text{Hom}_{\mathbb{R}}(N, P)) \\ &\cong \text{Hom}(X \otimes M \otimes N, P) \\ &\cong \text{Hom}(X \otimes N \otimes M, P) \\ &\cong \text{Hom}(X \otimes N, \text{Hom}_{\mathbb{R}}(M, P)) \\ &\cong \text{Hom}(X, \text{Hom}_{\mathbb{R}}(N, \text{Hom}_{\mathbb{R}}(M, P))) \end{aligned}$$

10

$$\left( \begin{aligned} &\text{could just do } \text{Hom}(M, \text{Hom}(N, P)) \\ &\cong \text{Hom}(M \otimes N, P) \\ &\cong \text{Hom}(N \otimes M, P) \\ &\cong \text{Hom}(N, \text{Hom}(M, P)) \end{aligned} \right)$$



□

② Is  $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{5})$  Galois?

Yes. since  $\mathbb{Q}$  is characteristic 0, it is separable.

For normal, we show every conjugate root is also in  $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{5})$ .

$i\sqrt{3}$  is a root of the quadratic  $x^2 + 3$ .

So  $-i\sqrt{3}$ , the other root, is also in the field.

$\sqrt[3]{5}$  is a root of  $x^3 - 5$ , and the other roots are  $\sqrt[3]{5}\omega$ ,  $\sqrt[3]{5}\omega^2$  for  $\omega$  a primitive cube root of unity.

Thankfully, we can take  $\omega = \frac{-1 + \sqrt{3}i}{2}$ ,

which is in the field, so the conjugate roots of  $\sqrt[3]{5}$  are in the field too, and it is normal. Thus, Galois.

✓

①

③ let  $F/k$  normal, algebraic. let  $f \in k[x]$  irreducible

If  $u, v$  are two roots of  $f$  in  $F$ , show there is a  $k$ -automorphism  $\sigma: F \rightarrow F$  with  $\sigma(u) = v$ .

We build  $\tilde{\sigma}: F \rightarrow \bar{k}$  as

$$\begin{array}{ccc} F & \xrightarrow{\tilde{\sigma}} & \bar{k} \\ \uparrow & & \uparrow \\ k(u) & \xrightarrow{u \mapsto v} & k(v) \\ \uparrow & & \uparrow \\ k & \longrightarrow & k \end{array}$$

by using  $u, v$  conjugate here and the nice extension theorems we have for maps of fields.

But since  $F/k$  is normal, any  $\tilde{\sigma}: F \rightarrow \bar{k}$  restricts to an automorphism  $\sigma: F \rightarrow F$ . As needed.

✓  
⑩

Chris Grossack

[C] (4) Let  $F$  be a subfield of  $\mathbb{C}$  with  $F/\mathbb{Q}$  finite, galois whose galois group  $G \cong A_5$ . Show  $F \cap \mathbb{Q}(e^{2\pi i/n}) = \mathbb{Q}$  for every  $n \geq 1$ .

we know  $\mathbb{Q}(e^{2\pi i/n}) = \mathbb{Q}(\zeta_n)$  is galois, since the conjugate roots are  $\zeta_n^k$  for  $1 \leq k \leq n$ .

So we have a diagram

$$\begin{array}{ccc} F & & \mathbb{Q}(\zeta_n) \\ & \searrow & / \\ & F \cap \mathbb{Q}(\zeta_n) & \\ & | & \\ & \mathbb{Q} & \end{array}$$

but the intersection of galois extensions is galois, ✓.

So we get a tower

where  $F \cap \mathbb{Q}(\zeta_n) / \mathbb{Q}$  is normal.

$$\begin{array}{c} F \\ | \\ F \cap \mathbb{Q}(\zeta_n) \\ | \\ \mathbb{Q} \end{array}$$

Then  $\text{gal}(F / (F \cap \mathbb{Q}(\zeta_n))) \triangleleft G$ , and so is either all of  $A_5$  or  $1$ , since  $G = A_5$  is simple. (8)

But  $F \neq F \cap \mathbb{Q}(\zeta_n)$ , so  $\text{gal}(F \cap \mathbb{Q}(\zeta_n) / \mathbb{Q}) = 1 = \text{gal}(\mathbb{Q} / \mathbb{Q})$  and by the galois correspondence,  $F \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ .

(5) Let  $K$  be a finite field,  $f \in K[x]$  monic irreducible.  
Prove  $f \mid x^{q^n} - x$  where  $|K| = q$  and  $n = \deg f$ .

Let  $\alpha$  be a root of  $f$  in some algebraic closure.

now  $K(\alpha) \cong \frac{K[x]}{f}$  has size  $q^n$  (since it's an  $n$ -dim vector space over  $K$ )

Now the multiplicative group  $K(\alpha)^\times$  has order  $q^n - 1$ .

So  $\alpha^{q^n - 1} = 1$  by group theory, and  $\alpha^{q^n} = \alpha$ .

So  $\alpha$  is also a root of  $x^{q^n} - x$ , and since

this is true of every root of  $f$  we see  $f \mid x^{q^n} - x$ .

explain:

use  $f$  is min. poly of its roots,  
or use  $f$  is separable so  
no repeated roots.

(8)