January 2015:

(7) — A, B, C R-mods; $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$,

prove that there is an R-mod hom. $j: C \to B$

such that $pj = 1_C$ iff there is an R-mod hom.

$q: B \to A$ such that $qi = 1_A$.

Hungerford IV.1.18.

Split (short exact) sequence: a sequence is split whenever there is a j as above. In particular this implies $B \cong A \oplus C$ as R-mods.
As long as we are in an abelian category, a short exact sequence splits iff the middle term is a direct sum of the others. Note that R-mod is an abelian category.

Steps:

1. Show that if such a j exists then $B \cong A \oplus C$.
2. Show that if $B \cong A \oplus C$, then there is a desired q.

1. The diagram:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[d, "1_A"'] & A\oplus C \arrow[r, "\pi_2"] \arrow[d, "f"] & C \arrow[r] \arrow[d, "1_C"] & 0 \\
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "p"] & C \arrow[r] & 0
\end{tikzcd}$$

Now since $j : C \to B$ is with $jp = 1_C$ and i is injective, we have a morphism $f : A\oplus C \to B$ given by $f(a,c) = i(a) + j(c)$.

Prove this or cite Hungerford IV.1.13.

By the Short Five Lemma, f is an R-iso.

Alternatively, diagram chase.

2. Say $f : A\oplus C \to B$ is R-iso. The diagram:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[d, "1_A"'] & A\oplus C \arrow[r, "\pi_2"] \arrow[d, "f"] & C \arrow[r] \arrow[d, "1_C"] & 0 \\
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r, "p"] & C \arrow[r] & 0
\end{tikzcd}$$

commutes. Define $q : B \to A$ as $q := \pi_1 f^{-1}$.

Now: $gi(a) = (\pi_1 f^{-1})(f \iota_1 i_A^{-1})(a) = (\pi_1 f^{-1} f \iota_1 i_A^{-1})(a) =$

$$= (\pi_1 \iota_1 1_A^{-1})(a) = (1_A 1_A^{-1})(a) = a.$$

8 - R comm. ring with 1, I prime ideal, $S = R \setminus I$. Prove that $S^{-1}R$ is local.

Hungerford III.4.11(ii).

Recall: A ring is local whenever it has a unique maximal ideal.

The ideals of R that are prime are exactly the prime ideals that are disjoint from S.

Let M be a maximal ideal of $S^{-1}R$. Then M is prime, so we can write $M = S^{-1}T$ for some prime ideal $T \subseteq R$, and also $T \subseteq I$. Hence $S^{-1}T \subseteq S^{-1}I$, and since $S^{-1}I \neq S^{-1}R$ with $S^{-1}T$ maximal, we must have $M = S^{-1}T = S^{-1}I$.

So $S^{-1}I$ is the unique maximal ideal of $S^{-1}R$.

August 2015:

① - Prove that there are at most four groups of order 306 containing an element of order 9.

This is a classification (of groups) problem. We should think about semidirect products and the like.

$|G| = 306 = 2 \cdot 9 \cdot 17 = 2 \cdot 3^2 \cdot 17.$

To keep in mind: having an element of order 9 says that G has a Sylow subgroup $\mathbb{Z}/(9)$.

By the Third Sylow Theorem we have: $n_3 = 1, 34$; $n_{17} = 1, 18$.

Since the Sylow-17-subgroup has prime order 17, it must be $\mathbb{Z}/(17)$.

The claim is that $n_{17} \neq 18$ and $n_3 \neq 34$. First, the intersection of any such subgroup and $\mathbb{Z}/(9)$ is trivial, moreover the intersection of any two of such subgroups must also be trivial. Second, suppose $n_{17} = 18$, then the non-identity elements are at least $16 \cdot 18 + 6 \cdot 34 = 492 > 306 = |G|$.

This means that there is always a unique Sylow-17 or unique Sylow-3 subgroup, which must be normal.

Suppose first $n_{17}=1$, call it $N_{17} \trianglelefteq G$. Given any Sylow-3-subgroup H_3, then the semidirect product $N_{17} \rtimes_\phi H_3 < G$, where

$$\phi: H_3 \longrightarrow \mathrm{Aut}(N_{17}), \quad \text{i.e. } \phi: \mathbb{Z}/(9) \longrightarrow \mathbb{Z}/(16).$$

Keep this in mind, we are not done yet.

Since $9 \nmid 16$, ϕ must be trivial. Hence $N_{17} \rtimes_\phi H_3 = N_{17} \times H_3 = \mathbb{Z}/(17) \times \mathbb{Z}/(9)$.

Suppose then $n_3=1$, $N_3 \trianglelefteq G$, by the same argument we want, for each Sylow-17-subgroup H_{17}, the semidirect product $N_3 \rtimes_\phi H_{17} < G$, so

$\phi: H_{17} \longrightarrow \mathrm{Aut}(N_3)$, where $|\mathrm{Aut}(N_3)|$ is not divisible by 17.

must also be trivial, hence: $N_3 \rtimes_\phi H_{17} = \mathbb{Z}/(9) \times \mathbb{Z}/(17)$.

We have a subgroup $N = \mathbb{Z}/(9) \times \mathbb{Z}/(17)$ with $[G:N]=2$, so $N \trianglelefteq G$.

Therefore for a Sylow-2-subgroup H_2 we have that $G \cong N \rtimes_\phi H_2$

for some $\phi : \underset{\underset{\mathbb{Z}/(2)}{\cong}}{H_2} \longrightarrow \mathrm{Aut}(N)$. Note that $\phi(1)$ has order 2,

and $\mathrm{Aut}(N) = \mathrm{Aut}(\mathbb{Z}/(9) \times \mathbb{Z}/(17)) = \underset{\underset{1}{\Downarrow}}{\mathbb{Z}/(2)} \times \mathbb{Z}/(3) \times \underset{\underset{8}{\Downarrow}}{\mathbb{Z}/(16)}$, so :

(i) $\phi(1) = (1,0,0)$,

(ii) $\phi(1) = (0,0,8)$,

(iii) $\phi(1) = (1,0,8)$,

(iv) ϕ trivial: $\phi(1) = (0,0,0)$.

Hence $G \cong N \rtimes_\phi H_2$ for at most four ϕ.

② - $A \in \mathbb{Z}^{n\times n}$ with (i,j) entry a_{ij}, $x = (x_1, \dots, x_n)$, define x^A to be

$(x_1^{a_{1,1}} \cdots x_n^{a_{n,1}}, \dots, x_1^{a_{1,n}} \cdots x_n^{a_{n,n}})$. Assume $x^{AB} = (x^A)^B$.

(a) Prove that when $\det(A) \in \{\pm 1\}$ and k field, then $m_A(x) := x^A$ defines an automorphism of $(k^\times)^n$.

Question to ask: what operations should we consider on $(k^\times)^n$?

Note: A has inverse $A^{-1} \in \mathbb{Z}^{n\times n}$ ⊛ Also xy is coordinate-wise multiplication.

Also for $x, y \in (k^\times)^n$, then :

$m_A(xy) = ((x_1y_1)^{a_{11}} \cdots (x_ny_n)^{a_{n1}}, \dots, (x_1y_1)^{a_{1n}} \cdots (x_ny_n)^{a_{nn}}) =$

$$= \left(x_1^{a_{11}} y_1^{a_{11}} \cdots x_n^{a_{n1}} y_n^{a_{n1}}, \ldots, x_1^{a_{1n}} y_1^{a_{1n}} \cdots x_n^{a_{nn}} y_n^{a_{nn}} \right) =$$

$$= \left(x_1^{a_{11}} \cdots x_n^{a_{n1}} y_1^{a_{11}} \cdots y_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdots x_n^{a_{nn}} y_1^{a_{1n}} \cdots y_n^{a_{nn}} \right) =$$

$$= \left(x_1^{a_{11}} \cdots x_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdots x_n^{a_{nn}} \right) \left(y_1^{a_{11}} \cdots y_n^{a_{n1}}, \ldots, y_1^{a_{1n}} \cdots y_n^{a_{nn}} \right) =$$

$$= m_A(x) m_A(y).$$

Note: $(x^A)^{A^{-1}} = x^{AA^{-1}} = x = x^{A^{-1}A} = (x^{A^{-1}})^A$, so $m_{A^{-1}}$ is the inverse of m_A. $\circledast$ $A^{-1} = \dfrac{\operatorname{adj}(A)}{\det(A)} = \pm \operatorname{adj}(A) \in \mathbb{Z}^{n \times n}$.

(b) For arbitrary $A \in \mathbb{Z}^{n\times n}$, m_A is an endomorphism of $U = \{-1,1\}^n \subseteq (\mathbb{Q}^\times)^n$.

Find and prove an explicit formula for the cardinality of the quotient group $U/\ker(m_A)$ as a function of the $\mathbb{Z}/(2)$-rank of the mod 2 reduction A.

Question to ask: what is this?

By definition, the $\mathbb{Z}/(2)$-rank of A is the rank of A mod 2.

Notice that $U = \{1,-1\} \times \overset{n}{\cdots} \times \{1,-1\}$.

The mod 2 reduction of $A \in \mathbb{Z}^{n\times n}$ is:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \longrightarrow A \bmod 2 = \begin{bmatrix} a_{11} \bmod 2 & \cdots & a_{1n} \bmod 2 \\ \vdots & & \vdots \\ a_{n1} \bmod 2 & \cdots & a_{nn} \bmod 2 \end{bmatrix}.$$

Then $\det(A \bmod 2) = \det(A) \bmod 2$.

$AB \bmod 2 = (A \bmod 2)(B \bmod 2)$.

What the problem is asking is to compute $|U/\ker(m_A)|$, and since $|U| = 2^n$, we only have to compute $|\ker(m_A)|$.

$m_A : U = \{1,-1\} \times \overset{n}{\cdots} \times \{1,-1\} \longrightarrow (\mathbb{Q}^\times)^n$, so we are looking at elements $u \in U$ such that $m_A(u) = (1,\dots,1)$.

$$u^A = (1,\dots,1).$$

$$\left((\pm 1)^{a_{11}} \cdots (\pm 1)^{a_{1n}}, \dots, (\pm 1)^{a_{n1}} \cdots (\pm 1)^{a_{nn}}\right) = (1,\dots,1)$$

An $u \in U$ is a solution u of $m_A(u) = (1,\dots,1)$ iff it is a solution of $m_{A \bmod 2}(u) = (1,\dots,1)$, because the only thing that matters is whether a_{ij} is odd or even.

Hence it suffices to look at:

$$m_{A \bmod 2} : U = \{1,-1\} \times \overset{n}{\cdots} \times \{1,-1\} \longrightarrow (\mathbb{Q}^\times)^n$$

Now magic happens: use the Smith factorization of A, which says

Something more "general" PAQ reduction

$A = PDQ$ where P, Q are invertible with $\det(P) = \pm 1 = \det(Q)$ and D is diagonal. Now we can replace the rank of A by the rank of D, i.e. we can use the rank of D instead of the rank of A (since P, Q are invertible). Moreover: $m_A(u) = m_Q(m_D(m_P(u)))$, and since P, Q are invertible, by (a) m_P, m_Q are automorphisms, so:

$$|\ker(m_A)| = |\ker(m_D)|.$$

Also, D diagonal means $D \bmod 2$ diagonal and: $D = \begin{bmatrix} d_{11} & & 0 \\ & \ddots & \\ 0 & & d_{nn} \end{bmatrix}$.

$$m_D(u) = (u_1^{d_{11}}, \dots, u_n^{d_{nn}}),$$ so the solutions to $m_D(u) = (1, \dots, 1)$ is given by those $u \in U = \{1,-1\} \times \overset{n}{\cdots} \times \{1,-1\}$ such that $u_i = 1$ whenever $d_{ii} = 1$, but $u_i = \pm 1$ whenever $d_{ii} = 0$.

Suppose $D \bmod 2$ has r ones in the diagonal, which is exactly $\operatorname{rank}(D \bmod 2) = \operatorname{rank}(A \bmod 2)$. Then $|\ker(m_D)| = 2^{n-r}$.

Hence: $\left| U/_{\ker(m_A)} \right| = \dfrac{|U|}{|\ker(m_A)|} = \dfrac{|U|}{|\ker(m_D)|} = \dfrac{2^n}{2^{n-r}} = 2^r$

where $r = \operatorname{rank}(A \bmod 2)$.

(3) - k field

(a) Given $v \in k^n$ non-zero, prove there is a basis $\{v, v_2, \dots, v_n\}$ of k^n.

Note $\{v\}$ is linearly independent. Since every linearly independent set is contained in a maximal linearly independent subset of k^n. But every

Hungerford IV.2.4.

maximal linearly independent subset of k^n is a basis of k^n, so this

Hungerford IV.2.3.

maximal linearly independent subset contains v and has n elements (since basis of k^n have exactly n elements), write it $\{v, v_2, \dots, v_n\}$.

Assumed as truth: 1. Every l.i. subset is contained in a maximal l.i. subset.
2. Every maximal l.i. subset is a basis.
3. Basis of k^n have exactly n elements.

(b) Whenever $k = \bar{k}$, prove that any $A \in k^{n \times n}$ can be written as $A = V^{-1} U V$ with $U, V \in k^{n \times n}$ with V invertible and U upper triangular.

This is the Jordan Canonical Form. Hungerford VII.4.7(iii).

Seeing $A \in k^{n\times n}$ as a linear transformation $A : k^n \longrightarrow k^n$ given by matrix-vector multiplication, writing $A = V^{-1}UV$ means that U is either considering the kernel or the cokernel of A, depending on whether U is upper or lower triangular.

Thm: When $k = \bar{k}$, a matrix $A \in k^{n\times n}$ is similar to a matrix J (i.e. there is an invertible matrix V such that $A = V^{-1}JV$) where J is a direct sum of the elementary Jordan matrices associated with a unique family of polynomials of the form $(x-b)^m$, $b \in k$. Also J is uniquely determined except for the order of the elementary Jordan matrices along its main diagonal.

$$J = \begin{bmatrix} \square & & & \\ & \square & & \\ & & \ddots & \\ & & & \square \end{bmatrix} = \begin{bmatrix} \square & & \\ & \ddots & \\ & & \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} \ddots & \\ & \square \end{bmatrix}.$$

(Proof in Hungerford VII.4.7(ii)).

④ - Given R-mod A, A', B, B', C, C' and R-hom $f, f', g, g', \alpha, \beta, \gamma$ with α, γ monomorphisms, and a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$

exact row

exact row

prove that β is a monomorphism.

Let $b \in B$ such that $\beta(b) = 0$. Since $g'\beta = \gamma g$ we have:

$0 = g'\beta(b) = \gamma g(b)$. Thus $g(b) = 0$ since γ is monomorphism.

Hence: $b \in \ker(g) = \operatorname{im}(f)$, so there is some $a \in A$ such that $f(a) = b$. Since $f'\alpha = \beta f$ we have:

$0 = \beta(b) = \beta f(a) = f'\alpha(a)$. Now f' is monomorphism by exactness of the bottom row, so $\alpha(a) = 0$. Since α is monomorphism we have $a = 0$. So $b = f(a) = f(0) = 0$.

⑤ - $p, q \in \mathbb{N}$, p prime, q prime power, $\mathbb{F}_q$ field with q elements.

(a) If $x^{p^n} - x - 1$ irreducible in $\mathbb{F}_p[x]$ then prove:

(i) $\phi(y) := y^{p^n}$ is automorphism of $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$.

(ii) $\phi^{(p)}$ is the identity map on $\mathbb{F}_p[x]/\langle x^{p} - x - 1\rangle$.

(i) The map $\phi : \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle \longrightarrow \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$ is an

$y \longmapsto y^{p^n}$

n-fold iteration of the map

$$\psi : \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle \longrightarrow \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle .$$
$$y \longmapsto y^p$$

If ψ is an automorphism, then $\phi = \psi^{(n)}$ is also an automorphism.

Notice that the characteristic of $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$ is p. (one way of seeing this is because $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$ is a field extension of $\mathbb{F}_p$, and then the characteristic must be preserved).

Hungerford V.1.6. Hungerford III.5.2.

This means that for all $y, z \in \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$ we have:

$$(yz)^p = y^p z^p \quad \text{and} \quad (y+z)^p = y^p + z^p .$$

This is good enough to check that ψ is a field homomorphism (not zero).

Injectivity comes from being in a field, surjectivity comes from being between finite sets. So ψ is an automorphism.

(ii) Since $x^{p^n} - x - 1$ is zero in $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$, we have that:

$$\phi(x) = x^{p^n} = x + 1 \quad \text{in } \mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle .$$

Also any $a \in \mathbb{F}_p$ satisfies $a^p = a$, Hungerford III.5.3.

$\psi(a) = a$

and thus $\phi(a) = a$.

<u>Claim</u>: ϕ satisfies $\phi^{(n)}(x) = x + n$ for all $n \in \mathbb{N}$. We saw true for $n=1$. Assume $\phi^{(j-1)}(x) = x + (j-1)$, to see the case $n=j$ notice:

$$\phi^{(j)}(x) = \phi(x + (j-1)) = \phi(x) + \phi(j-1) = x^{p^n} + (j-1)^{p^n} =$$

$$= (x+1) + (j-1) = x + j.$$

So by induction $\phi^{(p)}(x) = x + p = x$. This means that $\phi^{(p)}$ fixes x, so it must also fix $x^2, x^3, \dots, x^{p^n-1}$. Now $\{1, x, x^2, \dots, x^{p^n-1}\}$ form a basis of $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$ as $\mathbb{F}_p$-v.s. Hence $\phi^{(p)}$ fixes all the basis elements. We also saw ϕ fixes $\mathbb{F}_p$, thus $\phi^{(p)}$ also fixes $\mathbb{F}_p$. This adds up to $\phi^{(p)}$ fixing $\mathbb{F}_p[x]/\langle x^{p^n} - x - 1\rangle$, as desired.

(b) Suppose f irreducible in $\mathbb{F}_q[x]$, prove that f divides $x^{q^n}-x$ if and only if the degree of f divides n.

$\Rightarrow$) Suppose $f \mid x^{q^n}-x$. We know that $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n}-x$

Hungerford V.5.6.

(we are using that q is a prime power), since $|\mathbb{F}_{q^n}| = q^n$, $|\mathbb{F}_q| = q$,

so $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Take K the splitting field of f, since

$f \mid x^{q^n}-x$ we have $K \subseteq \mathbb{F}_{q^n}$. Since f is irreducible over $\mathbb{F}_q$

we must have $\mathbb{F}_q \subseteq K$. Then:

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K] \cdot \deg(f)$$

so $\deg(f) \mid n$.

$\Leftarrow$) Set $d = \deg(f) \mid n$, we first show that f divides $x^{q^d}-x$.

For this consider $\mathbb{F}_q[x]/\langle f \rangle$ a field of q^d elements. Then $x^{q^d} = x$

in $\mathbb{F}_q[x]/\langle f \rangle$, so f divides $x^{q^d}-x$.

Hungerford V.5.3.

Since $d | n$ means:

$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + \dots + q^{n-jd} + \dots + q^d + 1)$$

which implies $q^d - 1$ divides $q^n - 1$. We can write:

$$x^{q^n-1} - 1 = (x^{q^d-1} - 1)(x^{q^n-1-(q^d-1)} + x^{q^n-1-2\cdot(q^d-1)} + \dots +$$

$$+ x^{q^n-1-j(q^d-1)} + \dots + x^{q^d-1} + 1).$$

This yields that $x(x^{q^d-1} - 1)$ divides $x(x^{q^n-1} - 1)$

so f divides $x^{q^d} - x$, which in turn divides $x^{q^n} - x$.

(c) Prove that $x^{47^n} - x - 1$ is <u>not</u> irreducible in $\mathbb{F}_{47}[x]$ for $n \geq 2$.

Assume for a contradiction that $x^{47^n} - x - 1$ is irreducible over $\mathbb{F}_{47}[x]$.

Then by part (a) the map $\phi^{(47)}(y) = y^{47^{47n}}$ on (what should be a field $\mathbb{F}_{47}[x] / \langle x^{47^n} - x - 1 \rangle$) is the identity. Then:

$x^{47^{47n}} \equiv x \mod x^{47^n} - x - 1$, that is

$$x^{47^{47n}} - x \equiv 0 \mod x^{47^n} - x - 1,$$ that is

$x^{47^n} - x - 1$ divides $x^{47^{47n}} - x$.

Then by part (b) the degree of $x^{47^n} - x - 1$ divides $47n$.

This is a contradiction since $47^n \nmid 47n$ for $n \geq 2$.