August 2014:

(6) - H finite p-group acting on Σ finite.
$\Sigma_0 \subseteq \Sigma$ fixed points. Show that $|\Sigma| \equiv |\Sigma_0|$ mod p.

Lemma II.5.1. Hungerford.

Let $\{\bar{x}_1, \dots, \bar{x}_n\}$ be representatives of the orbits of the action $H \circlearrowright \Sigma$ with size over 1. Then:

$$|\Sigma| = |\Sigma_0| + |\bar{x}_1| + \cdots + |\bar{x}_n|$$

By the Order-Stabilizer theorem: $|\bar{x}_i| = [H : H_{x_i}] > 1$, since H is p-group, all subgroups have order divisible by p. So: $|\Sigma| - |\Sigma_0| = |\bar{x}_1| + \cdots + |\bar{x}_n|$ is divisible by p, so $|\Sigma| - |\Sigma_0| \equiv 0$ mod p.

(b) Prove Second Sylow Theorem.

Any two Sylow p-subgroups are conjugate.

Let H, P be two Sylow p-subgroups, $H \curvearrowright \underset{X}{\underset{\shortparallel}{G/P}}$ by translation.

The number of cosets: $|G/P| = [G:P]$, which is relatively prime to p. Then $p \nmid |G/P|$, so $|X_0| > 0$ by part (a). This means that a coset $aP \in G/P$ is fixed: $h(aP) = aP$ for all $h \in H$. Thus:

$$a^{-1}(h(aP)) = a^{-1}(aP) = P, \text{ which means } a^{-1}ha \in P$$

for all $h \in H$. So $a^{-1}Ha < P$, so since

$|a^{-1}Ha| = |H| = |P|$ we have $a^{-1}Ha = P$.

7 - F_1, F_2 f.d. G. extension fields of K with $F_i \subset \overline{K}$, $i=1,2$. Show $F_1 \cdot F_2$ is Galois over K.

Hungerford V.1.11. Finite dimensional extensions are finitely generated and algebraic.

So F_1/K, F_2/K are f.g. and algebraic.

Also, Galois and also f.d. over K, so Hungerford V.3.11. and following remark implies that there exist polynomials $f_1(x), f_2(x) \in K[x]$ with irreducible factors such that F_1, F_2 are the splitting fields of $f_1(x), f_2(x)$ respectively.

Thus $F_1 \cdot F_2$ is the splitting field of the least common multiple of $f_1(x), f_2(x)$. So by Hungerford V.3.11. we have that $F_1 \cdot F_2$ is Galois over K.

8 - R comm. ring satisfying the descending chain condition.

Show that every prime ideal in R is maximal.

We work with $R \ni 1$. <u>Trick:</u> look at R/P for P prime.

We want to use that P maximal iff R/P field.

We know that P prime iff R/P domain.

<u>Recall:</u> An ideal $I \subset R/P$ is of the form J/P for some ideal $J \subset R$. So this means that R/P also satisfies the descending chain condition. ← maybe be more explicit with details here.

Take an element $x \in R/P$, we want $x^{-1} \in R/P$. Consider:

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots \supseteq (x^n) \supseteq \cdots$$ is a descending chain in R/P.

It must stabilize: there is some i with $(x^i) = (x^j)$ for all $j > i$. In particular $(x^i) = (x^{i+1})$ so there is $y \in R/P$ such that $x^i = yx^{i+1}$, since P prime, R/P is domain so we can cancel: $1 = yx$ (and $1 = xy$) so $x^{-1} = y \in R/P$.

January 2015:

① -(a) G group, $A, B \leq G$ abelian. Prove $A \cap B \trianglelefteq \langle A \cup B \rangle$.

Thought process: $A \cap B$ should be commutative inside $\langle A \cup B \rangle$. So if we see $A \cap B \leq Z(\langle A \cup B \rangle) \trianglelefteq \langle A \cup B \rangle$, we are done.

Let $x \in A \cap B$, $g \in \langle A \cup B \rangle$, we want: $gx = xg$. Write:

$$g = a_1 b_1 \cdots a_n b_n \quad \text{with } a_i \in A,\ b_i \in B. \text{ Now:}$$

$$gx = a_1 b_1 \cdots a_n b_n x = a_1 b_1 \cdots a_n x b_n = \cdots =$$

$$= a_1 x b_1 \cdots a_n b_n = x a_1 b_1 \cdots a_n b_n = xg.$$

because $x \in A, B$ both abelian. Then $A \cap B \leq Z(\langle A \cup B \rangle)$,

so $A \cap B \trianglelefteq \langle A \cup B \rangle$.

(b) G finite group not cyclic of prime order (not $\mathbb{Z}/(p)$, for p prime) with every proper subgroup abelian. Prove G contains a nontrivial, proper, normal subgroup.

Since $|G|$ is not prime, by the Sylow Theorems we have a bunch of proper nontrivial subgroups of G (all of them are abelian because we are told so). Since G is finite, there is a proper nontrivial subgroup that is maximal with respect to inclusion H.

Look at $N_G(H)$, since H is maximal and $H < N_G(H)$ we have $N_G(H) = H$ or $N_G(H) = G$. If $N_G(H) = G$ then $H \trianglelefteq G$ and we are done. We are left with the case $N_G(H) = H$.

In particular $[G : N_G(H)] = [G : H] = \dfrac{|G|}{|H|}$ are the conjugates of H. Take $\bar{H}$ a conjugate of H, it must also be maximal

$$\Big(\bar{H} < M, \text{ then } \bar{H} = gHg^{-1} \text{ so } H = g^{-1}gHg^{-1}g =$$

$$= g^{-1}\bar{H}g \leq g^{-1}Mg = \bar{M}, \text{ contradiction with } H \text{ maximal}\Big)$$

If $H \cap \bar{H} \neq \{e\}$ then $\langle H \cup \bar{H} \rangle = G$ by maximality of

$H, \bar{H}$, and by (a) we have $\{e\} \neq H \cap \bar{H} \trianglelefteq \langle H \cup \bar{H} \rangle = G$.

What remains is $H \cap \bar{H} = \{e\}$. This must be the case for all conjugates of H (otherwise we are in the previous case).

The number of nonidentity elements in some conjugate of H is:

$$\frac{|G|}{|H|} \cdot (|H| - 1) = |G| - \frac{|G|}{|H|}.$$

Now since $|H| \geq 2$ because H nontrivial, we have:

$$\frac{|G|}{2} \leq |G| - \frac{|G|}{|H|} < |G| - 1.$$

So there is some nontrivial $x \in G$ that is not contained in any conjugate of H. Thus $\langle x \rangle$ is a proper nontrivial subgroup of G, so it is contained in some maximal nontrivial proper subgroup K that is not conjugate to H. We can assume (by doing the same argument as for H) that the intersection of K with any of its conjugates $\bar{K}$ is trivial: $K \cap \bar{K} = \{e\}$.

We now have two options: $\bar{H} \cap \bar{K} = \{e\}$ or $\bar{H} \cap \bar{K} \neq \{e\}$.

If $\bar{H} \cap \bar{K} = \{e\}$ then we must have:

$$|G| > \underbrace{|G| - \frac{|G|}{|H|}}_{\substack{\text{number of nonidentity} \\ \text{elements in some} \\ \text{conjugate of } H}} + \underbrace{|G| - \frac{|G|}{|K|}}_{\substack{\text{number of nonidentity elements} \\ \text{in some conjugate of } K}} \geq \frac{|G|}{2} + \frac{|G|}{2} = |G| \text{, contradiction.}$$

Finally, we find $\bar{H}, \bar{K}$ some conjugates of H, K that are maximal, so $\langle \bar{H} \cup \bar{K} \rangle = G$, and different, and $\bar{H} \cap \bar{K} \neq \{e\}$, so $\bar{H} \cap \bar{K}$ is a nontrivial, proper subgroup. By part (a) we have $\bar{H} \cap \bar{K} \trianglelefteq \langle \bar{H} \cup \bar{K} \rangle = G$.

② - $|G| = 45$, prove G abelian.

$|G| = 45 = 9 \cdot 5 = 3^2 \cdot 5$.

By Sylow 3 we have $n_5 = 1, 3, 9$ so $\underset{H}{n_5 = 1}$ so it is normal

and such subgroup is $\mathbb{Z}/(5)$, and $\underset{K}{n_3 = 1}$ so it is normal and

such subgroup is $\mathbb{Z}/(9)$ or $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

Any non-identity element in H or K have coprime orders, so

$H \cap K = \{e\}$. Now $|HK| = 45$, since $H, K \trianglelefteq G$ we have

$$HK = H \times K \leq G \quad \text{so} \quad H \times K = G.$$

Thus $G \cong \mathbb{Z}/(9) \times \mathbb{Z}/(5)$ or $G \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(5)$,

both abelian.

3 - R integral domain, Noetherian. Prove that if every two

$a, b \neq 0$ in R have a common divisor $xa + yb$, $x, y \in R$,

then R is a P.I.D.

Since R is Noetherian, every ideal is finitely generated Hungerford VIII.1.9.

So it suffices to prove that if $I \subseteq R$ is an ideal generated by n elements, then I is principal (i.e. generated by one element). Do induction.

<u>$n=1$:</u> Good.

Suppose hypothesis true for $n-1$: if an ideal can be generated by $n-1$ elements (or fewer) then it is principal.

<u>n:</u> Suppose $I = (a_1, \dots, a_n)$, an element $x \in I$ can be written

Ⓐ $\overset{?}{\vdash} = (r, a_3, \dots, a_n)$, r taking a_1, a_2.

Warning! claim: $I = \underbrace{(a_1, \dots, a_{n-1})}(a_n) \overset{?}{=} (s)(a_n) \overset{?}{=} (r, a_n) \overset{?}{=} (s)$

is dangerous to do!

$(a_1, \dots, a_{n-1}) = (d)$

as $x = r_1 a_1 + \dots + r_n a_n = \underbrace{(r_1 a_1 + \dots + r_{n-1} a_{n-1})}_{a} + r_n a_n$.

$x \in (d) + (a_n) = (s)$

claim

Note: What if $a = 0$?

By hypothesis, if $a \neq 0$, then a and a_n have a Ⓑ common divisor, call it $s = u a + w a_n$ for some $u, w \in R$.

Compare (s) with $(a) + (a_n)$, we want $(s) = (a) + (a_n)$.

This does <u>not</u> work as general as we need!

Rmk: $(a_1, \ldots, a_n) = (a_1) + \cdots + (a_n)$, but for this proving just $n=1$ is not good enough, we also need $\boxed{n=2}$

(i) Here proving $(d) + (a_n) = (s)$ is good enough for a solution.

(A) Reducing n to $n-1$. This does not require to prove $n=2$.

$n=2$: $I = (a,b)$. We know that $a, b \neq 0$, so they have

a common divisor $r = xa + yb$. The claim is

$(r) = (a,b)$. Clearly $r \in (a,b)$ so $(r) \subseteq (a,b)$. Now

↑ this is hard without explicit form!

since $r \mid a$ and $r \mid b$ we have $(a,b) \subseteq (r)$.

$s_1 a_1 + \cdots + s_n a_n \in (r, a_3, \ldots, a_n)$ and any element in $(r, a_3, \ldots, a_n)$ is in $(a_1, \ldots, a_n)$.

(4) - Prove that $x^4 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.

By Gauss' Lemma, if it is irreducible over $\mathbb{Z}$ it will be irreducible over $\mathbb{Q}$. How to proceed:

1. Show that it does <u>not</u> have a root.
   Hence if it decomposes, it must be as a multiplication of polynomials of degree 2.

2. Suppose it decomposes as a multiplication of polynomials of degree 2. Find contradiction by multiplying out.

Alternatively:

<u>Rmk</u>: A polynomial is reducible over $\mathbb{Z}$ implies that it is reducible over $\mathbb{Z}/(p)$ for all p prime.

So if a polynomial is irreducible over $\mathbb{Z}/(p)$ for some p prime, then it is irreducible over $\mathbb{Z}$.

Look at $p=3$ and proceed as before.

(5) - $f(x) = x^5 - 6x + 3$ over $\mathbb{Q}$, F its splitting field.

(a) Prove $f(x)$ irreducible.

Eisenstein's by $p=3$.

Roots of $f(x)$:

r_1, r_2, r_3, r_4, r_5.

(b) Prove $Gal(F/\mathbb{Q}) \leq S_5$.

Elements of the Galois group must permute roots of $f(x)$.

Since F is the splitting field of $f(x)$, it is generated by all the roots of $f(x)$. Note that any two $\alpha, \beta \in Gal(F/\mathbb{Q})$ such that $\alpha(r_i) = \beta(r_i)$ for all $i = 1, \dots, 5$ are equal.

necessary for injectivity

Associate each root r_i to a letter, we have 5 of them, each element of $Gal(F/\mathbb{Q})$ permutes them, since they are determined by their action on the roots, the map:

$$Gal(F/\mathbb{Q}) \xrightarrow{\phi} S_5$$

$$\alpha \longmapsto \phi(\alpha) \text{ permuting } 1, \dots, 5 \text{ as roots } r_1, \dots, r_5.$$

This ϕ is an injection.

(c) Prove that G contains a 5-cycle.

Let r be a root of $f(x)$. Then (since f is irreducible of degree 5) we have $[\mathbb{Q}(r), \mathbb{Q}] = 5$. Since $F/\mathbb{Q}$ is Galois we have $|G| = [F:\mathbb{Q}] = [F:\mathbb{Q}(r)][\mathbb{Q}(r):\mathbb{Q}]$ so $5 \mid |G|$.

Then we must have an element of order 5 by Cauchy's Theorem. Since $G \leq S_5$, the only elements of S_5 with order 5 are the 5-cycles, we must have that G has a 5 cycle.

(d) Prove that G contains a transposition.

Hint: $f(x)$ has exactly 3 real roots, so $f(x)$ has exactly 2 complex non-real roots.

Two of the roots are then of the form $a \pm ib$ with $b \neq 0$.

Then complex conjugation is an F-automorphism fixing $\mathbb{Q}$.

Real roots: r_1, r_2, r_3.

$$F \xrightarrow[\text{complex conjugation}]{\sigma} F$$

$$r_1 \longmapsto r_1$$
$$r_2 \longmapsto r_2$$
$$r_3 \longmapsto r_3$$
$$a+ib \longmapsto a-ib$$
$$a-ib \longmapsto a+ib$$

$$\begin{tikzcd} & F \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(r_1, r_2, r_3) \arrow[dr, dash] & & \mathbb{Q}(a \pm ib) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$$\mathbb{Q} \subseteq F \subseteq \mathbb{C} \xrightarrow{\overline{?}} \mathbb{Q} \subseteq F \subseteq \mathbb{C}$$

So complex conjugation σ is a transposition in $G \leq S_5$.

Roots:

$$\alpha, \beta, \gamma, \delta$$

$$\begin{tikzcd} K \arrow[d, dash] & (x-\alpha)(x-\beta)(x-\gamma)(x-\delta) \\ F \arrow[d, dash] & (x-\alpha)(x-\gamma) \\ \mathbb{Q} & \end{tikzcd}$$

(e) Determine G.

<u>Claim</u>: $G \cong S_5$. Because G has a 5-cycle and a transposition.

Rmk: One of the equivalent ways of generating S_n is having an n-cycle and a transposition.

Let σ be our 5-cycle, τ the transposition. There is some power of σ that sends any a to b, for $a, b \in \{1, \dots, 5\}$.

$$\tau = (i_1\, i_2)$$

$$\sigma = (a_1 a_2 a_3 a_4 a_5).$$
$$\sigma^2 = (a_1 a_3 a_5 a_2 a_4).$$
$$\sigma^3 = (a_1 a_4 a_2 a_5 a_3).$$
$$\sigma^4 = (a_1 a_5 a_4 a_3 a_2).$$
$$\sigma^5 = \mathrm{id}.$$

We may then assume that G contains a 5-cycle σ of the form $\sigma = (i_1\, i_2\, i_3\, i_4\, i_5)$. Since S_5 is generated by transpositions, it suffices to show that G has all transpositions. It is good enough to show G has $(i_1 i_2), (i_2 i_3), (i_3, i_4), (i_4 i_5)$ by taking $i_j < i_k$ for all $j < k$:

$$(i_j\, i_k) = (i_j\, i_{j+1})(i_{j+1}\, i_{j+2}) \cdots (i_{k-2}\, i_{k-1})(i_{k-1}\, i_k)(i_{k-2}\, i_{k-1}) \cdots$$

$\cdots (i_{j+1} i_{j+2})(i_{j+1}\ i_j)$.

$\tau = (i_1 i_2)$.

Well now: $(i_j\ i_{j+1}) = \sigma^{j-1} \tau \sigma^{-(j-1)}$ for $\sigma = (i_1 i_2 i_3 i_4 i_5)$

⑥ - Prove $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial over $\mathbb{Q}$.

We do this by showing that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, and thus by Hungerford V.3.14. it cannot be the splitting field of any polynomial over $\mathbb{Q}$.
We show that the minimal polynomial of $\sqrt[4]{2}$ has a non-real root, meaning that a root cannot be in $\mathbb{Q}(\sqrt[4]{2})$, so it cannot split in $\mathbb{Q}(\sqrt[4]{2})$. Then by definition $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal.

$$f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) =$$
$$= (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = x^4 - 2.$$
$$f(\sqrt[4]{2}) = 0.$$

(or use reduction to $\mathbb{Z}/(3)$).

This $f(x)$ is irreducible by Eisenstein's with $p = 2$.

Thus $f(x)$ is the minimal polynomial of $\sqrt[4]{2}$ and has $i\sqrt[4]{2}$ a non-real root.