Previous Algebra Prelim Solutions

August 24, 2019 Trevor Jack

1 Unsolved

- J06 2(c), 3, 4(b-d), 5
- A06 3, 5
- J07
- A07 5
- J08 2, 4
- J09 1, 3, 4
- A08
- A10 5
- J11 2
- A12 5
- J12 6
- J14 5

2 January 2006

1(a): Because $|A_6| = 360 = 2^3 \cdot 3^2 \cdot 5$, then its Sylow 2-subgroups are of order 8. Let n_2 be the number of Sylow 2-subgroups. Then by Sylow's Theorem, $n_2|45$ and $n_2 \equiv 1(\text{mod } 2)$ so that $n_2 \in \{1, 3, 5, 9, 15, 45\}$. The subgroup $\langle(1, 2, 3, 4)(5, 6), (1, 3)(5, 6)\rangle$ is one such order-8 subgroup. By Sylow's Theorem, every subgroup of order 8 will be a conjugate of this subgroup. We can form other such groups simply by using different values for these generators. Each subgroup is completely determined by the 4-cycle of the first generator. There are $6 \cdot 5 \cdot 4 \cdot 3$ ways to pick 4 values from 6 and since there are 8 ways to write the same 4-cycle (4 possible first values and 2 directions to write the cycle), then there are 45 distinct ways to write the 4-cycle. As these are unique subgroups and 45 is the most number of order-8 subgroups possible under Sylow's Theorem, we are done.

1(b): The generators listed above correspond to a rotation and a flip of the vertices of a square; that is, to the generators of D_4.

2(a): For any $a, b \in G$, $ab = ab(baba) = (abba)ba = ba$ since $baba = abba = 1$

2(b): By the Fundamental Theorem of Finite Abelian Groups, $G = Z_{p_1} \times ... \times Z_{p_n}$ where $p_1, ..., p_n$ are (not necessarily distinct) primes. The only group Z_p where each of its elements is its own inverse is Z_2, so the only possible order of G is a power of 2.

2(c):

3: Let $ab \in I$ and assume $a \notin I$. Then $J_a := \{r \in R : ra \in I\}$ contains b. Because I is an ideal, then $ia \in I$ for any $i \in I$ and any $a \in R$. Thus, $I \subset J_a$. If $I = J_a$, we are done. If I is a proper sub-ideal of J_a, then J_a is finitely generated: $J_a = (j_1, ..., j_k)$. Then let $b = s_1 j_1 + ... + s_k j_k$ for some $s_1, ..., s_k \in R$... ??
An ideal that is not finitely generated can sit inside an ideal that is finitely generated, so it is not clear from the fact that $I \subseteq J_a$ that $J_a = I$. For example, consider the polynomial ring $\mathbb{Z}[x_1, x_2, \ldots]$ in infinitely many indeterminates. The whole ring itself is generated by 1, but the ideal $(x_1, x_2, \ldots)$ is not finitely generated. This is where we got stuck too.

4(a): Let $h_1, h_2, h_3 \in Hom_k(V, W)$ and $a, b \in k$. Then if we define addition naturally by $(h_1+h_2)(v) = h_1(v)+h_2(v)$, we get that $h_1+(h_2+h_3) = (h_1+h_2)+h_3$ (associativity), $h_1 + h_2 = h_2 + h_1$ (commutativity), and $(-h_1)(v) = -h_1(v)$ (inverses/identity). If we define scalar multiplication naturally by $(ah_1)(v) = ah_1(v)$, we get from W being a k-vector space that $((a + b)h_1)(v) = (a + b)h_1(v) = ah_1(v) + bh_1(v) = (ah_1)(v) + (bh_1)(v)$ (vector distribution), $(a(h_1 + h_2))(v) = a(h_1(v) + h_2(v)) = ah_1(v) + ah_2(v) = (ah_1 + ah_2)(v)$ (scalar distribution), and $((ab)h_1)(v) = abh_1(v) = a(bh_1(v)) = (a(bh_1))(v)$ (group action).

(b): k-linear maps are determined by how they act on the basis elements of a vector space and the image of these basis elements forms a basis of the image of the map. Then $dim_k(Hom_k(V, W)) = |W|^{|V|}$.
$\dim(\mathrm{Hom}(V, W)) = \dim(V)\dim(W)$. The way I thought of it was that k-linear maps

can be represented by matrices. These matrices map V to W, so they must be matrices of size $|W| \times |V|$. This is a $|V||W|$-dimensional space.

5: Assume $x^p - x - a$ does not split over $K[x]$ so that there is some root $b \notin K$. Since K is of characteristic p, then by Freshman Exponentiation, $(b+c)^p - (b+c) - a = b^p + c^p - b - c - a = b^p - b - a + c^p - c$. So, anytime $c^p - c = 0$, then $(b+c)$ is a root of $x^p - x - a$. Now, $c^p - c = c(c^{p-1} - 1)$ so that the roots are zero and the roots of unity $\{\xi_1, ...\xi_{p-1}\}$. Then $x^p - x - a = (x-b)(x-(b+\xi_1))...(x-(b+\xi_{p-1}))$. Since $b \notin K$, then the splitting field of the minimum polynomial of b must also contain one of these roots. But an extension that contains one root must contain them all so that the minimum polynomial of b is $x^p - x - a$, which must then be irreducible. (Sort of an intuitive jump. I could use help filling in details here...)
We made zero headway on this problem, and I think we would really benefit from discussing it with you when you return.

6: The roots of f are $\{\sqrt[5]{3}e^{\frac{2n\pi i}{5}}\}_{n=0}^{4}$. Because $x^5 - 3$ is irreducible, it is the minimum polynomial for $\sqrt[5]{3}$ so that $|Q[\sqrt[5]{3}] : Q| = 5$. Because the fifth cyclotomic polynomial is the minimum polynomial for the fifth roots of unity and it is of degree-4, then $|Q[e^{\frac{2\pi i}{5}}, \sqrt[5]{3}] : Q| = 20$. By the Fundamental Theorem of Galois Theory, the Galois group is of order 20. The automorphisms that are elements of this group must send roots to roots, so they are determined by where they send the elements $\sqrt[5]{3}$ and $e^{\frac{2\pi i}{5}}$. The following two automorphisms generate the group: $r(\sqrt[5]{3}) = \sqrt[5]{3}$ and $r(e^{\frac{2\pi i}{5}}) = e^{\frac{4\pi i}{5}}$; $s(\sqrt[5]{3}) = \sqrt[5]{3}e^{\frac{2\pi i}{5}}$ and $s(e^{\frac{2\pi i}{5}}) = e^{\frac{2\pi i}{5}}$. Note that $r^4 = s^5 = e$ and $rs = s^2r$, giving us the presentation $\langle r, s | r^4 = s^5 = e, rs = s^2 r\rangle$.

3 August 2006

1: We assume for the sake of contradiction that there exists a simple G for distinct odd primes p and q such that $p < q$ and $pq > 15$. Since G is simple, Sylow's Theorem gives the following possible numbers of Sylow subgroups: $n_2 \in \{p, q, pq\}, n_p \in \{4, q, 2q, 4q\}, n_q \in \{2p, 4p\}$. If we assume $p = 3$ and $q > 5$, then $n_q = 12$ and thus $q = 11$ and $|G| = 132$. Since we have at least $3 \cdot 4 - 3 = 9$ distinct elements in Sylow-3 subgroups and 121 distinct elements in Sylow-11 subgroups, plus the identity, we have 131 of 132 elements already accounted for before considering the Sylow-2 subgroups, of which there are at least 3. Thus, $p > 3$ and $q > 5$ so that $n_p \neq 4$.

Let $n_p = 4q$. Then there are $4q(p-1)$ elements of order p, leaving only $4q$ elements of other order. But there are at least $2p(q-1)$ elements of order q and $2p(q-1) > 4q$. Similarly, if $n_q = 4p$, then we have $4p(q-1)$ elements of order q leaving only $4p$ elements of other orders. But there are at least $q(p-1)$ elements of order p and $q(p-1) > 4p$. So, $n_p \in \{q, 2q\}$ and $n_q = 2p$. I don't know how to rule out these cases.

2: First a lemma. If M is a maximal subgroup of G, then every conjugate gMg^{-1} is maximal. Let $gMg^{-1} < H$. Then $M < g^{-1}Hg$ so that by the maximality of M, $g^{-1}Hg = M$ or G. But this forces $H = gMg^{-1}$ or G so that gMg^{-1} is maximal. Note that if M is maximal and not normal, then M is its own normalizer. By the Orbit-Stabilizer theorem, the number of conjugates of M is $|G : M|$. Since each conjugate is maximal, then they intersect trivially, giving $|G : M|(|M|-1)+1 = |G|-|G : M|+1$ elements in the union of these conjugates. Since $|G : M|$ divides $|G|$, this total is at least $|G|/2+1$. Also, since $|G : M| \neq 1$, there must be an element outside of this union belonging to another maximal subgroup, for which we'd get another union of at least $|G|/2+1$ elements. But this is too many elements, so that some maximal subgroup cannot be its own normalizer, hence it is normal in G.

4: Because $Z[i]$ is a PID (in fact, it is a Euclidean Domain), then every ideal is of the form (z). Let (a) be prime and consider any $(a) \subset (z)$. Then $bz = a$ for some b and because (a) is prime, then $ac = b$ or $ac = z$. If $ac = b$, then $acz = a$ so that z is a unit and $(z) = Z[i]$. Otherwise, $(a) = (z)$ so that (a) is maximal. If (a) is maximal, then consider any $a = bz$ so that $(a) \in (z)$. Then either z is a unit so that $az^{-1} = b$ and a divides b or $(a) = (z)$ so that a divides z.

5: On the final... anyone have that solution handy?

6: The roots of this polynomial are $\{\sqrt[6]{3}e^{\frac{2k\pi i}{6}}\}_{k=0}^{5}$. $x^6 - 3$ is the minimum polynomial for $\sqrt[6]{3}$ so that $|Q(\sqrt[6]{3}) : Q| = 6$. The 6^{th} cyclotomic polynomial $(x - e^{\frac{2\pi i}{6}})(x - e^{\frac{10\pi i}{6}})$ is the minimum polynomial of the 6^{th} root of unity. Then for the Galois group G, we have $|G| = 12$. Define automorphisms r and s as: $r(\sqrt[6]{3}) = \sqrt[6]{3}e^{\frac{2\pi i}{6}}, r(e^{\frac{2\pi i}{6}}) = e^{\frac{2\pi i}{6}}, s(\sqrt[6]{3}) = \sqrt[6]{3}, s(e^{\frac{2\pi i}{6}}) = e^{\frac{10\pi i}{6}}$. The group presentation for this is $\{r, s | r^6 = s^2 = e, rs = sr^{-1}\}$ which is D_{12}.

4 August 2007

1: Let $|G| = 12$. By Sylow's Theorem, $|Syl_2(G)| \in \{1, 3\}$ and $|Syl_3(G)| \in \{1, 4\}$. If $|Syl_2(G)| = |Syl_3(G)| = 1$, then G is abelian and thus all elements commute. If $|Syl_3(G)| = 4$, then there are at least eight elements of order 3 and since there must be at least one Sylow-4 subgroup, there can be no elements of order 6. If $|Syl_2(G)| = 3$, then there are at least six elements of order 4, one element of order 2, one element of order 1, and two elements of order 3. Thus, there can only be two elements of order 6, which must lie in the same cyclic subgroup and must then commute.

2: By Sylow's Theorem, we know there are groups of order 3, 5, and 7. We further know that there are either 1 or 15 groups of order 7. If there's only 1, then it is normal; call it N. Then for any group of order 5, H, the group HN is a subgroup of order 35. If there are 15 groups of order 7, then 90 of the 105 elements are of order 7. By Sylow's Theorem, there are either 1 or 21 groups of order 5. But only 15 elements remain to be of order 5, so there must only be 1 group of order 5, which is then normal. So, again, HN is a subgroup of order 35. By Sylow's Theorem applied to this subgroup, there must be normal subgroups of orders 5 and 7 so that the subgroup is a direct product of subgroups of relatively prime order. Thus, the order 35 subgroup is cyclic and it's generator is of order 35.

3: Assume R is a UFD. Pick any $a, b \in R - \{0\}$ and let $a = u \cdot m_1 \cdot ... \cdot m_i$ and $b = v \cdot n_1 \cdot ... \cdot n_j$ be the unique factorizations of a and b into units u and v and irreducibles $m_1, ..., m_i, n_1, ...,$ and n_j. If b divides a, then $I_{a,b} = R = \langle 1 \rangle$. Otherwise, let $c = n_1 \cdot ... \cdot n_k$ be the product of irreducible divisors of b that do not divide a. If $x \in I_{a,b}$, then $ax = br$ for some $r \in R$. Because R is a UFD, x is a multiple of c. Furthermore, every multiple of c is in $I_{a,b}$, so that $I_{a,b} = \langle c \rangle$.

Now assume that R is not a UFD. Then there is some $b \in R$ with non-unique factorizations: $b = u \cdot m_1 \cdot ... \cdot m_i = v \cdot n_1 \cdot ... \cdot n_j$. Because the m's and n's are not units, then (WLOG) m_1 and n_1 do not appear in the other factorization. Let $a = m_1 \cdot n_1$. Then $x \in I_{a,b}$ if either x is a multiple of $m_2 \cdot ... \cdot m_i$ or $n_2 \cdot ... \cdot n_j$. These must be separate generators since $m_1 \neq n_1$, so $I_{a,b}$ is not principle.

4: It is equivalent to show that every submodule of M is finitely generated. Let $I \subseteq M$ be a submodule. Then $(I + N)/N \cong I/(I \cap N)$ by the second isomorphism theorem. Since $(I + N)/N \subseteq M/N$ and M/N is Noetherian, $(I + N)/N$ is finitely generated. Thus, $I/(I \cap N)$ is finitely generated, say $I/(I \cap N) = R\{u_1, u_2, \ldots, u_k\}$.

Also, $I \cap N \subseteq N$ and since N is Noetherian, $I \cap N$ is also finitely generated, say $I \cap N = R\{v_1, v_2 \ldots, v_\ell\}$. Let $x + (I \cap N) \in I/(I \cap N)$. Then $x + I \cap N = r_1u_1 + \cdots + r_ku_k + I \cap N$ for some $r_i \in R$, so $x = r_1u_1 + \ldots + r_ku_k + y$ for some $y \in I \cap N$. But $y = s_1v_1 + \cdots + s_\ell v_\ell$ for some $s_i \in R$, so $x = r_1u_1 + \cdots + r_ku_k + s_1v_1 + \cdots + s_\ell v_\ell$. Since $x \in I$ was chosen arbitrarily, the set $\{u_1, \ldots, u_k, v_1, \ldots, v_\ell\}$ generates I and I is finitely generated. Hence M is Noetherian.

5: ??

6: Let $f(x) = x^5 + 2x^4 + 5x^2 + x + 4$. Observe -2 is the only zero of $f(x)$ over F_{11} and $f(x) = (x+2)(x^4 + 5x + 2)$. Suppose that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Then $a = -c$, which gives $b + d = a^2$, $a(d - b) = 5$, and $bd = 2$, where equality is taken modulo 11. Since the squares modulo 11 are $1, 3, 4, 5, 9$, a^2 must take one of these values. A solution to these equations is $a = 5$, $b = 1$, $c = -5$, and $d = 2$, yielding $x^4 + 5x + 2 = (x^2 + 5x + 1)(x^2 - 5x + 2)$ over $_{11}$. Thus, the splitting field K of $f(x)$ over F_{11} is F_{11^4} and $Gal(K/F_{11}) = [K : F_{11}] = 4$ so that $(K/F_{11}) \cong Z/2Z \times Z/2Z$.

5 January 2008

1: Let $|G| = p^km$ where p does not divide m. Because G is non-abelian and simple, $m \neq 1$. Let $Syl_p(G)$ be the set of all Sylow-p subgroups. By Sylow's Theorem, G acts transitively on $Syl_p(G)$ by conjugation so that $\phi : G \to S_n$ according to how the elements of G permute the n elements of $Syl_p(G)$. Then because $ker(\phi) \triangleleft G$ and G is simple, then ϕ is injective. By Lagrange's Theorem, $|G|$ divides $|S_n| = n!$.

3: Pick any ideal I and pick $a \in I$ such that the GCD of a and any element in I that a doesn't divide is 1. That is, a has a minimal number of factors. Let b be any element I and consider (a, b). Since any ideal generated by two elements is principal, there exists $c \in I$ such that $(a, b) = (c)$. In other words, a can be written as a multiple of c, so $a = dc$ for some $d \in I$. But a has the minimal number of factors when compared to any element in I, so d must be a unit. Then $(c) = (a)$ so $b \in (a)$. Since b was an arbitrary element of I, we have $I \subseteq (a)$ and consequently $I = (a)$.

5: We first find the splitting field over F_2. $p(x) = x^4 + x^3 + 1$ is irreducible over F_2, so adjoining a root of $p(x)$ yields a degree-4 extension, F_{2^4}. For finite fields, adjoining any root of an irreducible polynomial adjoins all the roots so that F_{2^4} is the splitting field of $p(x)$ over F_2. So, the splitting field over F_{2^5} must contain both F_{2^4} and F_{2^5}.

The smallest such field is $F_{2^{20}}$.

6(i): False. Consider the field $F_2(x)$ and the extension $F_2(x)[\sqrt{x}] \cong F_2(x)[y]/(y^2-x)$. Since $y^2 - x = (y - \sqrt{x})(y - \sqrt{x})$ if F_2, then $y^2 - x$ is not separable so that the field extension is not Galois.

6(ii): True. The algebraic closure of F_p is the union of the fields F_{p^k} for all $k \in Z_{\geq 1}$, which is certainly infinite. And the algebraic closure of F_{p^k} for any $k \in Z_{\geq 1}$ is equal to the algebraic closure of F_p, since F_{p^k} is algebraic over F_p.

6 January 2009

2: Since p does not divide $(m-1)!$ nor m, then $p > m$ so that the only divisor of m that is congruent to 1 mod p is 1. Thus, by Sylow's Theorem, there is a single Sylow p-subgroup. Since Sylow subgroups conjugate into each other, this single group must be normal so that G is not simple. ("nonabelian" is unnecessary information)

3: Assume I is a prime ideal. If $I = I_1 \cap I_2$, then clearly $I \subset I_1$ and $I \subset I_2$. Assume there is some $a \in I_1$ that is not in I. Then pick any $b \in I_2$ and note that $ab \in I_1 \cap I_2 = I$. Since I is a prime ideal and $a \notin I$, then $b \in I$ so that $I_2 \subset I$, proving the first property. We prove the second by induction. Clearly, if $a \in I$ then $a \in I$. Assume $a^{n-1} \in I$ implies that $a \in I$. Because I is a prime ideal, then $a^n \in I$ forces either $a \in I$ or a^{n-1}, the latter of which again forces $a \in I$ by the induction hypothesis.

For the other direction... uh...

5: Pick any polynomial $p(x) = k_m x^m + ... + k_0$ so that $p'(x) = mk_m x^{m-1} + ... + k_1$. Then $d(p(l)) = d(k_m l^m) + ... + d(k_0)$. Since $d(k) = 0$ for all $k \in K$ and $d(k_i l^i) = d(k_i) l^i + k_i d(l^i)$, then $d(p(l)) = k_m d(l^m) + ... + k_1 d(l)$. Note that $d(l^m) = d(l) l^{m-1} + l d(l^{m-1})$ so that, by induction, $d(l^m) = m l^{m-1} d(l)$. Thus, $d(p(l)) = (k_m m d(l^{m-1}) + ... + k_1) d(l) = p'(l) d(l)$. Now pick any $l \in L$ and let $p(x) \in K[x]$ be the minimum polynomial of l. Because L is a separable extension, l cannot also be a root of $p'(x)$. Then $0 = d(0) = d(p(l)) = p'(l) d(l)$, which forces $d(l) = 0$.

6: Let $x = \sqrt{2+\sqrt{2}}$, then $x^2 = 2 + \sqrt{2}$, $(x^2-2)^2 = 2$, and so x is a root of $x^4 - 4x^2 + 2$, which is irreducible over Q by Eisenstein's Criterion. Then $Q[\sqrt{2+\sqrt{2}}/Q$

is a degree-4 extension. Note also that the other three roots are contained in this extension: $-\sqrt{2+\sqrt{2}}$ (obviously), $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2+\sqrt{2}}^2-2}{\sqrt{2+\sqrt{2}}}$, and $-\sqrt{2-\sqrt{2}}$ (from the previous root). Thus, the polynomial splits over $Q[\sqrt{2+\sqrt{2}}]$ so that the extension is Galois. The following automorphism is of order-4, finishing the proof: $\phi(a+b\sqrt{2+\sqrt{2}}) = a+b\sqrt{2-\sqrt{2}}$.

7 August 2009

1(a): D_{48}
1(b): If G is nilpotent, then there is a lower central series $G \triangleright [G,G] \triangleright [[G,G],G] \triangleright ... \triangleright 1$ that ends with the trivial group after a finite number of terms. Since $\phi([G,G]) = [\phi(G), \phi(G)]$ then applying the homomorphism $\phi : \{H | H < G\} \rightarrow \{H/N | H/N < G/N\}$ to the lower central series yields a lower central series for G/N, proving that no such example exists.
1(c): $\{e,s\}$, $\{e,sr\}$, $\{e,sr^2\}$, $\{e,sr^3\}$, and $\{e,sr^4\}$ are the 5 Sylow 2-subgroups of D_{10}.

2(a): For any $x \in X$, let $a \in Stab(x)$ and pick any $b \in G$. Then because G is abelian, $ab(x) = ba(x) = b(x)$ so that a stabilizes any element in the orbit of x. Since the action of G on X is transitive, then $Orb(x) = X$ so that $Stab(x) = Stab(y)$ for every $x, y \in X$. Then (x, y_1) and (x, y_2) are in different orbits if $y_1 \neq y_2$, which thus gives us $|X|$ orbits.

2(b): For any $x \in X$, the action of G on $Orb(x)$ is transitive. Thus by the above result, (x, y_1) and (x, y_2) are in different orbits if $y_1 \neq y_2$ and $y_1, y_2 \in Orb(x)$. Then the sum of the sizes of the orbits represents the number of orbits of $X \times X$ under the action of G. This sum is precisely $|X|$.

3: For any $r \in R$, (r^2) is a principal ideal and thus prime. Since $r^2 = r \cdot r$, then r^2 divides r so that there is some r^{-1} such that $r^{-1}r^2 = r$. Thus, R is a field.

4(a): First note that $F_{q^m} \cong F_q[x]/(x^m + a_{m-1}x^{m-1} + ... + a_0)$ for some irreducible polynomial. Then we let x act on $GL_m(F_q)$ as a linear transformation that has the following rational canonical form:

$$\begin{pmatrix} 0 & ... & ... & -a_0 \\ 1 & \ddots & ... & -a_1 \\ 0 & \ddots & ... & \vdots \\ \vdots & ... & ... & \vdots \\ ... & ... & ... & -a_{m-1} \end{pmatrix}$$

The identity $1 \in F_{q^m}$ corresponds to the $m \times m$ identity matrix. Then every other element of F_{q^m} corresponds to a matrix formed from an appropriate combination of 1 and x. Substituting these matrices into the top-left $m \times m$ block of the $n \times n$ identity matrix gives the desired injective homomorphism into $GL_n(F_q)$.

4(b): Let $F_9 \cong F_3[x]/(x^2+1)$ so that the rational canonical form for x is:

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Together with the identity matrix, we can obtain corresponding matrices for all eight elements of $F_9^{\times}$.

5: Let $q = p * k$ and f be of degree $m \leq k$. Then $F_p[x]/(f) \cong F_{p^m}$. If h and g are irreducible factors of f over F_q, then $F_q[x]/(h) \cong F_{p^m} \cong F_q[x]/(g)$ since we're adjoining to F_q a root of h or g which must also be a root of f. Then if $h = p^i$ and $g = p^j$, we get that $F_{p^i} \cong F_q[x]/(h) \cong F_q[x]/(g) \cong F_{p^j}$ so that $i = j$.

6(a): By Galois Theory, the Galois group $Gal(E/F)$ has a maximal subgroup $Gal(E/M)$, which must then be normal since it would be the only subgroup of its order. If $|Gal(E/F)| = p_1^{k_1} \cdot ... \cdot p_i^{k_i}$, then by Sylow's Theorem, there must be Sylow subgroups of orders $p_1^{k_1}$, ..., and $p_i^{k_i}$. Because $Gal(E/M)$ contains each of these groups, then $|Gal(E/M)$ is divisible by each of these prime powers so that $|Gal(E/M)| = |Gal(E/F)|$. But then it would not be a proper subgroup. So, $Gal(E/F)$ has a prime power order and thus $|E : F|$ is a prime power.

(b): Pick any $a \in Gal(E/F)$ such that $a \notin Gal(E/M)$. Then $(a) \not\subset Gal(E/M)$ so that (a) must be all of $Gal(E/F)$. Since it is cyclic, its subgroup lattice is a single chain of subgroups so that, for any distinct pair of subgroups, one of the subgroups will contain the other. By Galois Theory, the corresponding fields have the same structure and thus corresponding inclusion relations.

8 January 2010

1: Because K is normal, then $gkg^{-1} \in K$ for any $g \in G$. For $a, b \in G$, let $aka^{-1} = k^{\alpha}$ and $bkb^{-1} = k^{\beta}$. Then $abkb^{-1}a^{-1} = ak^{\beta}a^{-1} = (aka^{-1})^{\beta} = k^{\alpha\beta} = bk^{\alpha}b^{-1} = baka^{-1}b^{-1}$. Then for any $ghg^{-1}h^{-1} \in [G, G]$, $ghg^{-1}h^{-1}khgh^{-1}g^{-1} = ghh^{-1}g^{-1}kghh^{-1}g^{-1} = k$ so that $[G, G] \subset C_G(K)$. Since this holds for any cyclic subgroup of G, then the elements of $[G, G]$ commute with every element of G so that $[[G, G], G] = \{1\}$.

2: An automorphism can be defined by how it acts on generators. For there to be exactly two automorphisms, there must only be two generators to permute. If the order of the group is divisible by a prime $p > 3$, then it has a subgroup of order p, which has $p - 1$ generators and thus too many automorphisms. If the group has two subgroups of order 3, the subgroups must be distinct cyclic subgroups giving us four generators of order 3 and thus too many automorphisms. If the group has two subgroups of order 2, then the group contains a subgroup isomorphic to the Klein four group, which has six automorphisms (three elements of order 2, so 3! permutations of these generators). The dihedral group of order 6 has at least three automorphisms corresponding to conjugation by s, r, and r^2. This narrows our list to the following groups: Z_3, Z_4, and $Z_2 \times Z_3$.

3: Let I be a prime ideal so that R/I is an integral domain. Pick a nonzero $r \in R/I$ and note that $r^{n_r} = r$ gives us $r(r^{n_r} - 1) = 0$ so that $r^{-1} = r^{n_r - 1}$, making R/I a field. Then I must also be maximal.

4: Let A be the $n \times n$ matrix over $\mathbb{Q}$ whose entries are all equal to 1. Suppose φ is the associated linear transformation represented by A with respect to the basis $\mathcal{E} = \{e_1, e_2, \ldots, e_n\}$. Note that for all i we have $\varphi(e_i) = e_1 + e_2 + \ldots + e_n$. Thus rewriting the matrix A under the basis $\{\sum_{i=1}^{n} e_i, \sum_{i=1}^{n-1} e_i, \ldots, e_1 + e_2, e_1\}$ yields,

$$A' = \begin{bmatrix} n & n-1 & \ldots & 2 & 1 \\ 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 \end{bmatrix}.$$

Since the determinant of similar matrices is the same the characteristic polynomial of A is $\det(xI - A') = x^{n-1}(x - n)$. Putting the matrix $xI - A'$ into Smith-Normal

Form yields

$$\begin{bmatrix} 1 & & & & \\ & x & & & \\ & & \ddots & & \\ & & & x & \\ & & & & x(x-n) \end{bmatrix}.$$

Note that the last invariant factor $x(x-n)$ gives the minimal polynomial. Now if the characteristic of $\mathbb{F}$ divides n then the minimal polynomial reduces to x^2. Thus the elementary divisors are $x, \ldots, x, x^2$ where there are $n-2$ factors of x. The corresponding Jordan Canonical Form is given by the $n \times n$ matrix

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 0 & 0 \end{bmatrix}.$$

If the characteristic of $\mathbb{F}$ does not divide n then the minimal polynomial is $x(x-n)$ so the elementary divisors are $x, \ldots, x, x-n$ where there are $n-1$ factors of x. The corresponding Jordan Canonical Form is given by the $n \times n$ matrix

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & n \end{bmatrix}.$$

5: If either $\mathbb{F}[\sqrt[p]{a}]$ or $\mathbb{F}[\sqrt[p]{b}]$ are trivial extensions of $\mathbb{F}$ then clearly $\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}] = \mathbb{F}[\sqrt[p]{a} + \sqrt[p]{b}]$ so we may assume $\mathbb{F}[\sqrt[p]{a}]$ and $\mathbb{F}[\sqrt[p]{b}]$ are nontrivial extensions. Since $\mathbb{F}$ is a field whose characteristic is not p which contains a primitive pth root of unity then $\mathbb{F}$ contains all of the pth roots of unity and $\mathbb{F}[\sqrt[p]{a}]$ is a cyclic extension over $\mathbb{F}$ of degree p. Similarly $\mathbb{F}[\sqrt[p]{b}]$ is a cyclic extension over $\mathbb{F}$ of degree p. Then the composite $\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}]$ of these cyclic extensions is an abelian extension over $\mathbb{F}$.
Since $\mathbb{F}[\sqrt[p]{a} + \sqrt[p]{b}]$ is a subfield containing $\mathbb{F}$ of $\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}]$ then $\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}]$ is a Galois extension over $\mathbb{F}[\sqrt[p]{a} + \sqrt[p]{b}]$ by the Fundamental Theorem of Galois Theory. Any automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}]/\mathbb{F}[\sqrt[p]{a} + \sqrt[p]{b}])$ is completely determined by what it does to the generators $\sqrt[p]{a}$ and $\sqrt[p]{b}$ which must be sent to a pth root of a and a pth root of b respectively. Thus if ζ_p is a primitive pth root of unity then σ is defined by

$\sigma(\sqrt[p]{a}) = \zeta_p^k \sqrt[p]{a}$ and $\sigma(\sqrt[p]{b}) = \zeta_p^l \sqrt[p]{b}$ for some $0 \leq k, l < p$. Since σ must fix $\sqrt[p]{a} + \sqrt[p]{b}$ then,

$$\begin{aligned} \sigma(\sqrt[p]{a} + \sqrt[p]{b}) &= \sigma(\sqrt[p]{a}) + \sigma(\sqrt[p]{b}) \\ &= \zeta_p^k \sqrt[p]{a} + \zeta_p^l \sqrt[p]{b} \\ &= \sqrt[p]{a} + \sqrt[p]{b}. \end{aligned}$$

Thus $(\zeta_p^k - 1)\sqrt[p]{a} + (\zeta_p^l - 1)\sqrt[p]{b} = 0$. Since $\mathbb{F}[\sqrt[p]{a}] \neq \mathbb{F}[\sqrt[p]{b}]$ then $\sqrt[p]{a}$ and $\sqrt[p]{b}$ are linearly independent so $k = l = 0$. This implies σ is the identity automorphism, hence $\text{Gal}(\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}]/\mathbb{F}[\sqrt[p]{a}+\sqrt[p]{b}]) = 1$ is the trivial group. Thus $|\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}] : \mathbb{F}[\sqrt[p]{a}+\sqrt[p]{b}]| = 1$ so $\mathbb{F}[\sqrt[p]{a}, \sqrt[p]{b}] = \mathbb{F}[\sqrt[p]{a} + \sqrt[p]{b}]$.

6: By the Fundamental Theorem of Galois Theory, we can show the polynomial is not solvable by radicals if the Galois group of the splitting field of the polynomial over the base field is not solvable. If we can show that the Galois group is S_5, then we are done since the only normal subgroup of S_5 is the simple group A_5. S_5 is generated by any pair of a 5-cycle and a 2-cycle. By Eisenstein's Criterion, the polynomial is irreducible so that adjoining a root of the polynomial yields a degree-5 extension. Then the splitting field is an extension with degree divisible by 5 so that its Galois group has order divisible 5. By Cauchy's Theorem, the group has an order-5 subgroup, thus corresponding to a 5-cycle.

We can prove there is a 2-cycle by proving there is at least one pair of complex roots so that complex conjugation is a nontrivial automorphism. Note that $f(-2) = -22, f(0) = 2, f(1) = -1$, and $f(2) = 26$ so that f has zeroes in the intervals $(-2, 0), (0, 1)$, and $(1, 2)$. Furthermore, $f'(x)$ only has two real zeroes at $\pm\sqrt[4]{\frac{4}{5}}$, so there can only be three real roots. The Fundamental Theorem of Algebra guarantees we can find all the roots in C, so the other two must be complex.

9 August 2010

1: (a) Let H be a subgroup of index 6 and consider the action of left multiplication of A_6 on the cosets of A_6/H. By definition the stabilizer of H in A_6 of this action is $\text{Stab}_{A_6}(H) = \{\sigma \in A_6 \mid \sigma H = H\} = \{\sigma \in A_6 \mid \sigma \in H\} = H$. Now the stabilizer is the set of even permutations that fix H and permute the other five cosets of A_6/H, namely $\sigma_1 H, \sigma_2 H, \sigma_3 H, \sigma_4 H, \sigma_5 H$. Therefore,

$$H = \text{Stab}_{A_6}(H) = A_{\{\sigma_1 H, \sigma_2 H, \sigma_3 H, \sigma_4 H, \sigma_5 H\}} \cong A_5.$$

(b) Let G be a simple group of order $60 = 2^2 \cdot 3 \cdot 5$. Then $n_5 = 6$ so consider the action of conjugation of G on the six Sylow 5-subgroups. This action affords a permutation representation $\varphi : G \to S_6$. The kernel of φ is a normal subgroup of G and since G is simple $\ker \varphi$ must be trivial. Thus $G \leq S_6$. Because G is simple G also contains no subgroup of index 2, so in fact $G \leq A_6$. Then G is a index 6 subgroup of A_6 so by part (a), $G \cong A_5$.

2: Consider the homomorphism induced by θ given by $\bar{\theta} : G/N \to \theta(G)/\theta(N)$ where $gN \mapsto \theta(g)\theta(N)$. Then since the commutator subgroup of G/N is itself we have, $\theta(G)/\theta(N) = \bar{\theta}(G/N) = \bar{\theta}[G/N, G/N] = [\bar{\theta}(G/N), \bar{\theta}(G/N)] = [\theta(G)/\theta(N), \theta(G)/\theta(N)]$. Since $\theta(G)/\theta(N)$ is equal to its commutator subgroup the derived series of $\theta(G)/\theta(N)$ is just $\theta(G)/\theta(N)$. Since $\theta(G)$ is a subgroup of a solvable group H then $\theta(G)$ is solvable. Because the quotient groups of solvable groups are solvable then $\theta(G)/\theta(N)$ is also solvable. This implies the derived series of $\theta(G)/\theta(N)$ must eventually be 1. Thus $\theta(G)/\theta(N) = 1$ so that $\theta(G) = \theta(N)$ as desired.

3: Note $k[x, y, z]$ is an integral domain so prime elements are irreducible. Since $k[x, y, z]/\langle x \rangle \cong k[y, z]$ is an integral domain then x is prime and therefore irreducible. Similarly y and z are prime and irreducible elements.

Now the coset representatives of $k[x, y, z]/\langle xy - z^2 \rangle$ are finite sums of monomial terms of the form $ax^n y^m z^l$ for $a \in k$. If $n \geq m$ then $ax^n y^m z^l = (xy)^m x^{n-m} z^l = x^{n-m} z^{2m+l} \in k[x, z]$. Similarly if $n \leq m$ then $ax^n y^m z^l = (xy)^n y^{m-n} z^l = y^{m-n} z^{2n+l} \in k[y, z]$. Therefore,

$$k[x, y, z]/\langle xy - z^2 \rangle = \{f(x, z) + g(y, z) + \langle xy - z^2 \rangle \mid f \in k[x, z], g \in k[y, z]\} \cong k[x, z] + k[y, z].$$

Since $k[x, z]$ and $k[y, z]$ are integral domains it follows that $k[x, y, x]/\langle xy - z^2 \rangle$ is also an integral domain.

4: Since two matrices are in the same conjugacy class if and only if they have the same rational canonical form, it suffices to determine the rational canonical forms of a matrix in $SL(2, p)$. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, p).$$

Then $\det A = ad - bc = 1$. Calculating the characteristic polynomial of A yields

$$c_A(x) = \det xI - A = (x - a)(x - d) - bc = x^2 + (a + d)x + ad - bc = x^2 + (a + d)x + 1.$$

Thus the characteristic polynomial is determined by the coefficient of the linear term. Because we are working over the field with p elements then there are p different choices for the characteristic polynomial. If the characteristic polynomial is the same as the minimal polynomial then the minimal polynomial is the only invariant factor in the rational canonical form of A. This gives rise to a list of p different invariant factors whose corresponding rational canonical form is a representative for a conjugacy class of $SL(2,p)$.

If the characteristic polynomial is not the same as the minimal polynomial then the minimal polynomial must divide the characteristic polynomial, implying the characteristic polynomial must be reducible. Thus $c_A(x) = x^2 \pm 2 + 1 = (x \pm 1)^2$. Then $x+1, x+1$ and $x-1, x-1$ are two lists of invariant factors whose corresponding rational canonical forms represent two more conjugacy classes of $SL(2,p)$. Therefore there are a total of $p+2$ conjugacy classes of $SL(2,p)$.

5:

6(a): Note 0 and 1 are not roots of $f(x)$ so f does not contain a linear factor. If f is reducible then f must be the product of two irreducible quadratics. Since the polynomial $x^4 - x$ is precisely the product of all the distinct irreducible polynomials in $F[x]$ of degree d where d runs through all divisors of 4 then the irreducible quadratics over F are the divisors of $(x^4 - x)/(x(x-1))$ which gives the polynomial $x^2 + x + 1$. But $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$ so f cannot be the product of two irreducible quadratics. Thus f is irreducible in $F[x]$.

6(b): Since $f(x)$ is irreducible of degree 4 then $F[x]/(f(x)) = F_{2^4}$ is the splitting field of $f(x)$ over F. Since f the splitting field of f over E must be an extension of E then the splitting field must contain E. Since a finite field $F_{p^d} \subseteq F_{p^n}$ if and only if d divides n then the smallest field containing F_{2^4} and F_{2^5} is $F_{2^{20}}$. Hence $F_{2^{20}}$ is the splitting field of f over E.

10 January 2011

1: The presentation of $Z/4Z \times Z/2Z$ is $\{a, b | a^4 = b^2 = aba^{-1}b^{-1} = 1\}$, which is the same presentation for the following subgroup of S_7: $\langle(1,2,3,4),(5,6)\rangle$. Similarly, $Z/2Z \times Z/2Z \times Z/2Z \cong \{a, b, c | a^2 = b^2 = c^2 = aba^{-1}b^{-1} = aca^{-1}c^{-1} = bcb^{-1}c^{-1} = 1\} \cong \langle(1,2),(3,4),(5,6)\rangle$ and $D_8 \cong \{r, s | r^4 = s^2 = rsrs = 1\} \cong \langle(1,2,3,4),(1,3)\rangle$.

Every element in the symmetric group can be represented by a product of disjoint cycles and the order of a product of disjoint cycles is the least common multiple of the length of those cycles, since the cycles commute. The generator for $Z/8Z$ is an order-8 element. If 8 is the least common multiple of some product of numbers, then one of those numbers must be 8, which means an element of the symmetric group has order-8 only if it has an 8-cycle as one of the disjoint cycles. But no such cycle exists in S_7.

If $Q_8 < S_7$, then Q_8 acts on a set A of seven elements. By the Stabilizer-Orbit theorem, $|A| = |Stab_{Q_8}(a)| \cdot |Orb_{Q_8}(a)|$ for any $a \in A$. By Lagrange's Theorem, $|Stab_{Q_8}(a)|$ divides $|Q_8| = 8$. Since $|Stab_{Q_8}(a)|$ divides both 7 and 8, then for each $a \in A$, only the identity stabilizes a. Because there are only seven elements of A, then by the pigeon-hole principle, there are distinct elements $q_1, q_2 \in Q_8$ such that $q_1(a) = q_2(a)$. But then $q_2^{-1} \circ q_1$ fixes a so that $q_2^{-1} \circ q_1$ is the identity. And since inverses are unique, the elements can not be distinct. Thus, Q_8 does not act on a set of seven elements so that Q_8 is not a subgroup of S_7.

2: By Sylow's Theorem, every group of order 20, G, has a subgroup of order 4, which is isomorphic to either $Z/4Z$ or $Z/2Z \times Z/2Z$, and a subgroup of order 5, which is isomorphic to $Z/5Z$. The number of subgroups of order 5 divides 4 and is congruent to 1 mod 5. Then there must be one subgroup of order 5 and, since Sylow groups conjugate into one another, then this subgroup is normal. So, $G \cong Z/5Z \rtimes_\phi Z/4Z$ where $\phi : Z/4Z \to Aut(Z/5Z)$ or $G \cong Z/5Z \rtimes_\phi Z/2Z \times Z/2Z$ where $\phi : Z/2Z \times Z/2Z \to Aut(Z/5Z)$. Note that $Aut(Z/5Z) \cong Z/4Z$ and that the semidirect product is determined by which automorphism the generators of $Z/4Z$ and $Z/2Z \times Z/2Z$ are sent to.

If the generators are sent to the trivial automorphism in each case, we get the abelian groups $Z/20Z$ and $Z/2Z \times Z/10Z$, respectively. If $\phi(1) = 2$, we get the presentation $\{a, b | a^5 = b^4 = 1, b^{-1}ab = a^2\}$. If $\phi(1) = 3$, we get $\{a, b | a^5 = b^4 = 1, b^{-1}ab = a^3\} = \{a^4, b | (a^4)^5 = b^4 = 1, b^{-1}a^4b = a^2\}$ and is thus an isomorphic duplicate of the previous presentation. If $\phi(1) = 4$, we get $\{a, b | a^5 = b^4 = 1, b^{-1}ab = a^{-1}\}$. The generators for $Z/2Z \times Z/2Z$ are of order 2 so that they must be sent to either the trivial automorphism or to the order-2 element. Sending both to the trivial automorphism yields the abelian group above. Sending exactly one generator to the order-2 element yields $\{a, b | a^{10} = b^2 = 1, b^{-1}ab = a^{-1}\} = D_{20}$. Sending both yields $\{a, b, c | a^5 = b^2 = c^2 = 1, bab = cac = a^{-1}, bc = cb\} = \{abc, b | (abc)^{10} = b^2 = 1, b(abc)b = (abc)^{-1}\} = D_{20}$.

The following elements are of order 10: $2 \in Z/20Z$, $(0,1) \in Z/2Z \times Z/10Z$, $a \in D_{20}$, and $ab^2 \in \{a, b | a^5 = b^2 = 1, b^{-1}ab = a^{-1}\}$. It remains to show that $\{a, b | a^5 = b^4 = 1, b^{-1}ab = a^2\}$ has no element of order 10. Is there a fast way to do this? Reply: We did not find a good way to show that there is no element of order 10.

3: Assume that the conclusion is false and let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of counterexample ideals. Since R is Noetherian, there is an integer $n \geq 1$ for which $I_n = I_m$ for each $m \geq n$. Let $I = I_n$. Then I is a counterexample ideal, so $I \neq R$. Also, I is not prime, so there exist ideals $J, K \subseteq R$ properly containing I such that $JK \subseteq I$. By maximality of I, there exist prime ideals $P_1, \ldots, P_k$ and $Q_1, \ldots, Q_\ell$ for which each $P_i \supseteq J$, each $Q_i \supseteq K$, $P_1 \cdots P_k \subseteq J$ and $Q_1 \cdots Q_\ell \subseteq K$. Then each P_i and each Q_i is contained in I and $P_1 \cdots P_k Q_1 \cdots Q_\ell \subseteq I$, a contradiction. The result now follows.

4: We can prove by induction that the diagonalized form of $Ix - A$ is the identity matrix with the lower right most entry equal to $(x-1)^n$. The base case is certainly true: $[x-1]$. Assume that we can row reduce as follows:

$$\begin{pmatrix} x-1 & ... & -1 & -1 \\ \vdots & \ddots & \vdots & -1 \\ 0 & ... & x-1 & -1 \\ 0 & ... & 0 & x-1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & ... & 0 & -1 \\ \vdots & \ddots & \vdots & -1 \\ 0 & ... & (x-1)^{n-1} & -1 \\ 0 & ... & 0 & x-1 \end{pmatrix}$$

We need to reduce all but the last entry of the last column to zero. For all but the last two, we can achieve this by adding to the last column all but the last two columns, leaving us with:

$$\begin{pmatrix} 1 & ... & 0 & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & ... & (x-1)^{n-1} & -1 \\ 0 & ... & 0 & x-1 \end{pmatrix}$$

Now swap the last two columns, add $(x-1)R_{n-1}$ to R_n, add $(x-1)^{n-1}C_{n-1}$ to C_n, and multiply C_{n-1} by -1 to obtain:

$$\begin{pmatrix} 1 & ... & 0 & 0 \\ \vdots & \ddots & \vdots & 0 \\ 0 & ... & 1 & 0 \\ 0 & ... & 0 & (x-1)^n \end{pmatrix}$$

So, the rational canonical form of A can be determined from the invariant factor $(x-1)^n = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}x^k$ and the Jordan canonical form from the eigenvalue 1:

$$R = \begin{pmatrix} 0 & ... & 0 & (-1)^{n+1}\binom{n}{n} \\ 1 & 0 & \vdots & (-1)^n\binom{n}{n-1} \\ \vdots & \ddots & 0 & \vdots \\ 0 & ... & 1 & \binom{n}{1} \end{pmatrix}, J = \begin{pmatrix} 1 & 1 & ... & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & ... & 1 & 1 \\ 0 & ... & ... & 1 \end{pmatrix}$$

Because the minimum polynomial of A is degree n, then no nonzero linear combination of A^k's with every $k < n$ can equal zero.

5: We have

$$F = \bigcup_{j=1}^{\infty} F_{2^j}.$$

So for any $x \in F^\times$, there is some $j \in Z_{\geq 1}$ for which $x \in F_{2^j}^\times$. Thus, the order of any element in F divides $2^j - 1$ for some positive integer j. An element x of n is an n^{th} root of unity so that there are exactly $\varphi(n)$ elements of this order.

6(i): The minimum polynomial for $e^{\frac{2\pi i}{12}}$ is the 12^{th} cyclotomic polynomial $(x - e^{\frac{2\pi i}{12}})(x - e^{\frac{10\pi i}{12}})(x - e^{\frac{14\pi i}{12}})(x - e^{\frac{22\pi i}{12}}) = x^4 - x^2 + 1$. So, the Galois group for the extension $Q(e^{\frac{2\pi i}{12}})/Q$ are the automorphisms that fix Q and permute the roots of the above polynomial: $\phi_e(e^{\frac{2\pi i}{12}}) = e^{\frac{2\pi i}{12}}$, $\phi_a(e^{\frac{2\pi i}{12}}) = e^{\frac{10\pi i}{12}}$, $\phi_b(e^{\frac{2\pi i}{12}}) = e^{\frac{14\pi i}{12}}$, and $\phi_c(e^{\frac{2\pi i}{12}}) = e^{\frac{22\pi i}{12}}$. Note that ϕ_a and ϕ_b are each order-2 and that $\phi_c = \phi_a \circ \phi_b$, giving this group the structure of the Klein group $Z/2Z \times Z/2Z$.

(ii): By the Fundamental Theorem of Galois Theory, the field structure of a Galois extension matches the subgroup structure of the corresponding Galois group. Since the only subgroups of the Galois group above are $\{e, \phi_a\}$, $\{e, \phi_b\}$, and $\{e, \phi_c\}$, we need only determine what fields are fixed by ϕ_a, ϕ_b, and ϕ_c. Note the roots can be written as $\pm\sqrt{3} \pm \frac{i}{2}$ and that $\phi_a(\sqrt{3}) = \sqrt{3}$, $\phi_b(i) = i$, $\phi_c(\sqrt{3}i) = \phi_c(\sqrt{3})\phi_c(i) = (-\sqrt{3})(-i) = \sqrt{3}i$. Then the fixed fields of each are $Q(\sqrt{3})$, $Q(i)$, and $Q(\sqrt{3}i)$, respectively, which must be the only nontrivial subfields of $Q(e^{\frac{2\pi i}{12}})$.

11 August 2011

1: Let $g \in G$. Suppose $C_G(g) = Z(G)$. Then $g(G)$ and so $Z(G) = C_G(g) = G$, a contradiction. Thus $Z(G) < C_G(g)$ and so $|G : C_G(g)|$ is a proper divisor of $|G : Z(G)| = n$. Hence, $|cl_G(g)| = |G : C_G(g)| \leq n/2$.

2(a): Let $t = (t_{i,j}) \in T_n(F)$ and define $d = (t_{1,1}, t_{2,2}, \ldots, t_{n,n})$ and $u = (u_{i,j})$ by

$$u_{i,j} = \begin{cases} t_{i,j}t_{j,i}^{-1} & : i < j \\ 1 & : i = j \\ 0 & : j < i \end{cases}$$

Then $d \in D_n$, $u \in U_n$ and $t = ud$. Therefore, $T_n = U_nD_n$. Also $U_n \cap D_n = 1$ and it is given that $U_n \lhd T_n$. By the recognition theorem for semidirect products, $T_n = U_n \rtimes D_n$.

(b): Let q be a prime such that q divides $|T_n|$. Let $k = [F : F_p]$. Then $U_n = p^{kn(n-1)/2}$ and $D_n = (p^k - 1)^n$. If $q = p$, then $U_n \in Syl_p(T_n)$. Also, $U_n \lhd T_n$, so U_n is the unique Sylow q-subgroup of T_n and $Syl_q(T_n) = 1 = p^0$. Now assume that $q \neq p$ and let $Q \in Syl_q(D_n)$. Since diagonal matrices commute, D_n is abelian and $Q \lhd D_n$. Thus, $D_n \leq N_{T_n}(Q)$. Then since $|T_n| = (p^k - 1)^n p^{kn(n-1)/2)}$, $N_{T_n}(Q) = p^m(p^k - 1)^n$ for some nonnegative integer m. By the Orbit-Stabilizer theorem applied to the action of T_n on $Syl_q(T_n)$, we have that $|Syl_q(T_n)| = |T_n|/|N_{T_n}(Q)| = p^{kn(n-1)/2)-m}$.

3: Using the norm $N(x + \sqrt{pq}y) = x^2 - pqy^2$, note that because $x^2 \not\equiv \pm p (\bmod q)$, then no element in $Z[\sqrt{pq}]$ can have a norm of $\pm p$. Consider any elements $a, b \in Z[\sqrt{pq}]$ such that $ab = \sqrt{pq}$. Then $N(a)N(b) = N(ab) = N(\sqrt{pq}) = -pq$. Because $N(a), N(b) \neq \pm p$, then either $N(a) = \pm 1$ or $N(b) = \pm 1$, so that either a or b is a unit. Thus, $\sqrt{pq}$ is irreducible. And we are given that p and q are prime and thus irreducible. But then $pq = \sqrt{pq}\sqrt{pq}$ which are factorizations of a common element into different irreducibles so that $Z[\sqrt{pq}]$ is not a unique factorization domain.

4: Let M be a $\mathbb{Z}[i]$ module of size 100. By the Fundamental Theorem of Finitely Generated modules over a PID, there exists $r \geq 0$, $\alpha_i \in \mathbb{Z}_{\geq 1}$ and primes $p_i \in \mathbb{Z}[i]$ such that

$$M = \mathbb{Z}[i]^r \oplus \mathbb{Z}[i]/(p_1^{\alpha_1}) \oplus \mathbb{Z}[i]/(p_2^{\alpha_2}) \oplus \cdots \oplus \mathbb{Z}[i]/(p_k\alpha_k).$$

Since $M = 100$, we must have $r = 0$ and $\prod_{i=1}^{k} N(p_i)^{\alpha_i} = 100$, where $N(a+bi) = a^2+b^2$ is the usual norm. Note that $100 = 2^2 5^2 = (1+i)^2(1-i)^2(1+2i)^2(1-2i)^2 = (1+i)^4(2i+1)^2(2i-1)^2$. Since there are 5 partitions of 4 and 2 partitions of 2, it follows that there are $5 \cdot 2 \cdot 2 = 20$ choices for M and they are:

1. $\big(\mathbb{Z}[i]/(1+i)^4\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

2. $\big(\mathbb{Z}[i]/((1+i)^3\big) \oplus \mathbb{Z}[i]/(1+i) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

3. $\big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

4. $\big(\mathbb{Z}[i]/((1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

5. $\big(\mathbb{Z}[i]/((1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

6. $\big(\mathbb{Z}[i]/(1+i)^4\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

7. $\big(\mathbb{Z}[i]/((1+i)^3\big) \oplus \mathbb{Z}[i]/(1+i) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

8. $\big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

9. $\big(\mathbb{Z}[i]/((1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

10. $\big(\mathbb{Z}[i]/((1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)^2\big)$

11. $\big(\mathbb{Z}[i]/(1+i)^4\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

12. $\big(\mathbb{Z}[i]/((1+i)^3\big) \oplus \mathbb{Z}[i]/(1+i) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

13. $\big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

14. $\big(\mathbb{Z}[i]/((1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

15. $\big(\mathbb{Z}[i]/((1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)^2\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

16. $\big(\mathbb{Z}[i]/(1+i)^4\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

17. $\big(\mathbb{Z}[i]/((1+i)^3\big) \oplus \mathbb{Z}[i]/(1+i) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

18. $\big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

19. $\big(\mathbb{Z}[i]/((1+i)^2\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

20. $\big(\mathbb{Z}[i]/((1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(1+i)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i+1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big) \oplus \big(\mathbb{Z}[i]/(2i-1)\big)$

5: Write $F = F_p$ and $E = F_{p^m}$ for some prime p and $m \geq 2$. Then $\sigma : E \to E$ is the Frobenious automorphism, $u \mapsto u^p$. To show $N_{E/F} : E^\times \to F^\times$ is surjective, we must show $|ker(N_{E/F})| = (p^m - 1)/(p - 1)$. Now, from the given theorem, $ker(N_{E/F}) = \{u \in E | v/\sigma(v) = u \text{ for some } v \in E\}$. Since $\sigma(v) = v^p$, it suffices to find the order of the image of the homomorphism $\xi : E^\times \to E^\times$, $v \mapsto v^{p-1}$. Now F is the fixing field of σ, so $v^{p-1} = 1$ if and only if $v \in F^\times$. Hence $ker\xi = F^\times$ and $|im(N_{E/F})| = \frac{E^\times}{|ker(N_{E/F})|} = \frac{|E^\times|}{|E^\times/ker\xi|} = \frac{p^m-1}{(p^m-1)/(p-1)} = p - 1$. Thus, $im(N_{E/F}) = F^\times$ and $N_{E/F} : E^\times \to F^\times$ is surjective.

6(a): By Gauss's Lemma, a polynomial that is irreducible over integer coefficients is also irreducible over rational coefficients. Assume $x^3+x^2-2x-1 = (x+a)(x^2+bx+c)$ for some $a, b, c \in Z$. Then $a + b = 1$, $ab + c = -2$, and $ac = -1$. If $a = 1$, then $b = 0$ and $c = -1$. But then $ab + c \neq -2$. If $a = -1$, then $b = 2$ and $c = 1$. But again, $ab + c \neq -2$. Thus, there is no linear factor of $f(x)$.

(b): $f(x^2 - 2) = (x^2 - 2)^3 + (x^2 - 2)^2 - 2(x^2 - 2) - 1 = x^6 - 5x^4 + 6x^2 - 1 = (x^3 + x^2 - 2x - 1)(x^3 - x^2 - 2x + 1) = f(x)(x^3 - x^2 - 2x + 1)$

(c): By the result in part b, $f(\alpha^2 - 2) = f(\alpha)(\alpha^3 - \alpha^2 - 2\alpha + 1) = 0$. Now if $\alpha = \alpha^2 - 2$, then $\alpha = 2$ or $\alpha = -1$, but we can simply check that neither of these are roots of $f(x)$. Repeating this process yields $(\alpha^2 - 2)^2 - 2$ as a root. There are no rational roots to either $(\alpha^2 - 2)^2 - 2 = \alpha^2 - 2$ or $(\alpha^2 - 2)^2 - 2 = \alpha$. Thus, we have three distinct roots of $f(x)$ that exist in $Q[\alpha]$, so that $f(x)$ splits, making $Q[\alpha]/Q$ a normal field extension.

12 January 2012

1(a): False. Let $G = S_5$, let $P = \langle(1, 2, 3, 4, 5)\rangle$ and let $H = \langle(1, 3, 2, 4, 5)\rangle$. Observe $P \in_5 (G)$, H is the unique Sylow 5-subgroup of H and $1 = P \cap H \notin_5 (G)$.

1(b): True. Let $Q \in Syl_p(H)$. Then $Q \leq P$ for some $P \in Syl_p(G)$ and so $Q \leq P \cap H$. Since every element of P has p-power order, every element of $P \cap H$ has p-power order and so $P \cap H$ is a p-group. Hence $|P \cap H| \leq |Q|$ since $Q \in Syl_p(H)$. Thus, $|P \cap H| = |Q|$ and it follows that $Q = P \cap H$. In particular, $P \cap H \in Syl_p(H)$. Observe that if $x \in H \cap N_G(P)$, then $x(P \cap H)x^{-1} = xPx^{-1} \cap xHx^{-1} = P \cap H$ and so $x \in N_H(P \cap H)$. In particular, we have $|H \cap N_G(P)| \leq |N_H(P \cap H)|$. Now, let H act on $Syl_p(G)$ by conjugation. Since $_H(P) = H \cap N_G(P)$, the orbit-stabilizer theorem implies $|Syl_p(G)| \geq |H : Stab_H(P)| \geq |H : N_H(P \cap H)| = |Syl_p(H)|$.

2(a): First, notice that if G is abelian, then G is Camina. In this case, $[G, G] = 1$ and $Z(G) = G$, so $[G, G] \leq Z(G)$ and $Z(G) \not\leq [G, G]$. So assume that G is non-abelian. Let $x \in Z(G)$. Then $cl_G(x) = \{x\} \neq x[G, G]$ as $[G, G] \neq 1$. So we must have $x \in [G, G]$ and $Z(G) \leq [G, G]$. However, the other inclusion does not always hold. For example, A_4 is Camina: $[A_4, A_4] = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ and the conjugacy classes of elements in $A_4 \setminus [A_4, A_4]$ are $\{a, b, c, d\}$ and $\{a^2, b^2, c^2, d^2\}$ where $a = (1, 2, 3)$, $b = (1, 4, 2)$, $c = (1, 3, 4)$ and $d = (2, 4, 3)$. Since $Z(A_4) = 1$, we do not have $[A_4, A_4] \leq Z(A_4)$.

2(b): Let $g \in G \setminus [G, G]$ and let $x \in G$. Then $x^{-1}gx = g(g^{-1}x^{-1}gx) \in g[G, G]$. So $cl_G(g) \subseteq g[G, G]$. Therefore $|cl_G(g)| \in \{1, p\}$. However, g is not central as $Z(G) = [G, G]$, so $|cl_G(g)| = p$ and $cl_G(g) = g[G, G]$.

3(a): Let $a \in R \setminus \{0\}$. Then there exists $b \in R$ for which $ba = 1$. Since $b \neq 0$, there exists $c \in R$ for which $cb = 1$. So we have $c = c(ba) = (cb)a = a$. Hence every nonzero element of R has a multiplicative inverse and R is a division ring.

3(b): First, assume that R is a division ring. Let $S \subseteq R$ be any nonzero left R-submodule of R and let $a \in S$. Since $a \in R$, there exists $r \in R$ for which $ra = 1$. Since S is a R-submodule of R, $1 = ra \in S$, whence $S = R$. Now, assume that R is not a division ring and let $a \in R \setminus (R^\times \cup \{0\})$. Then $1 \notin Ra$, so $Ra \neq R$. Also, $a \in Ra$, so $Ra \neq \{0\}$. So R contains a nontrivial left R-submodule and is therefore not irreducible.

3(c): First, suppose that every nonzero left R-module has a submodule isomorphic to the left R-module R. Since every left R-submodule of the left R-module R is a left R-module, it follows that R is the only nonzero left R-module of R. Hence R is a division ring by (b). Now, assume that R is a division ring, let V be any nonzero left R-module and let $v \in V \setminus \{0\}$. Consider the map $\phi : R \to V$, $r \mapsto rv$. Since $\phi(r + s) = (r + s)v = rv + sv = \phi(r) + \phi(s)$ and $\phi(rs) = (rs)v = r(sv) = r\phi(s)$ for each $r, s \in R$, ϕ is a module homomorphism. Let $r \in ker\phi$. Then $rv = 0$, so r does not have a left inverse in R. But R is a division ring, which forces $r = 0$. Hence R is isomorphic to a submodule of V, by the first isomorphism theorem.

4(a): Let $\omega \in F_{p^2} \setminus F_p$. Then $\omega^2 \in F_p$ as $|F_{p^2}| : F_p = 2$ and the set $\{1, \omega\}$ is a basis for the vector space $_{p^2}$ over F_p. Now, let $\alpha = a + b\omega \in F_{p^2}^\times$ and consider the linear transformation $A : F_{p^2} \to F_{p^2}$, $v \mapsto \alpha v$. Since $A(1) = \alpha$ and $A(\omega) = b\omega^2 + a\omega$, the matrix form of A is $A = \left(\begin{smallmatrix} a & b\omega^2 \\ b & a \end{smallmatrix}\right)$. Also $\det A = a^2 - b^2\omega^2 = (a + b\omega)(a - b\omega) \neq 0$, as $ab^{-1} \notin \{\pm\omega\}$ in case $b \neq 0$ and $a^2 \neq 0$ in case $b = 0$. Therefore, we get a map $\phi :^{\times}_{p^2} \to G$, $a + b\omega \mapsto \begin{pmatrix} a & b\omega^2 \\ b & a \end{pmatrix}$.

It is clear that φ is injective. Let $a + b\omega, c + d\omega \in F_{p^2}^{\times}$. Then $\varphi\big((a + b\omega)(c + d\omega)\big) = \varphi(ac + bd\omega^2 + (bc + ad)\omega) = \begin{pmatrix} ac + bd\omega^2 & (bc + ad)\omega^2 \\ bc + ad & ac + bd\omega^2 \end{pmatrix} = \begin{pmatrix} a & b\omega^2 \\ b & a \end{pmatrix} \begin{pmatrix} c & d\omega^2 \\ d & c \end{pmatrix} = \varphi(a + b\omega)\varphi(c + d\omega)$, so that φ is also a homomorphism. The first isomorphism theorem now implies that $F_{p^2}^{\times} \leq G$, as claimed. Since $F_{p^2}^{\times}$ is cyclic of order $p^2 - 1$, $F_{p^2}^{\times}$ has an element of order $p^2 - 1$, and, therefore, so does G.

5: Since F_q is Galois over F_p, we have $T(x) = \sum_{\sigma \in (F_q/F_p)} \sigma(x)$. Note that for $x, y \in F_q$, $T(x+y) = \sum_\sigma \sigma(x+y) = \sum_\sigma \big(\sigma(x) + \sigma(y)\big) = \sum_\sigma \sigma(x) + \sum_\sigma \sigma(y) = T(x) + T(y)$. Now, if $p = 2$, then the map $\tau : F_q \to F_q$, $x \mapsto x^2$ is the Frobenius automorphism. So $x - x^2 = x - \tau(x)$ and $T(x - x^2) = T(x) - T(x^2) = T(x) - \sum_\sigma \sigma(\tau(x)) = T(x) - \sum_\sigma \sigma(x) = T(x) - T(x) = 0$. Hence, $T(x^2) = T(x)$ for every $x \in_q$.

Assume that $p \neq 2$ and let $\tau : F_q \to F_q$, $x \mapsto x^p$. Define $f : F_q \to F_q$ by $f(x) = x - \tau(x)$, and note that this is F_p-linear. Write $q = p^k$. Since F_p is the fixed field of τ, $\dim(\ker f) = 1$, so $\dim(\operatorname{im} f) = k - 1$. Now, from the above argument, $\operatorname{im} f \subseteq \ker T$. Observe also that $T(x) = 1 + x^p + x^{p^2} + \cdots + x^{p^{k-1}}$, since $(F_q/F_p) = \langle \tau \rangle$. Therefore, $T(x) = 0$ for at most p^{k-1} elements. So in fact, $\ker T = \operatorname{im} f$.
Now, consider $-1 \in F_p$. Then $-2 = -1 - (-1)^2 \neq 0$. So $-2 \neq x - \tau(x)$ for any $x \in F_p$. Also if $-2 = x - \tau(x)$, this would imply that $0 = \tau(x) - \tau(\tau(x))$, so that $\tau(x) \in F_p$. But then if $x \notin_p$, this would violate the injectivity of τ. Hence $-1 - (-1)^2 \neq x - \tau(x)$ for any $x \in_q \setminus_p$ either. Thus, $T(-1 - (-1)^2) \neq 0$.

6: By Eisenstein's Criterion, f is irreducible over $\mathbb{Z}$, hence over Q. Let K be the splitting field of f over Q. Then 5 divides $|K : Q|$. Also, since the discriminant is a square, $G = Gal(K/F) \leq A_5$. Now, S_5 has no subgroups of order 15 (as these are cyclic) and no subgroup of order 30 since A_5 is simple. Also, G cannot have a subgroup of order 20, i.e. of index 3, since $|A_5| = 60$ does not divide 3! and A_5 is simple. Also, $G \neq A_5$, since A_5 is not solvable. Thus, the only possibilities are $G \cong Z/5Z$ or $G \cong D_{10}$, since S_5 does not have a cyclic subgroup of order 10. Now, $f'(x) = 5x^4 + 11$, which has no real roots. So $f(x)$ must have exactly one real zero. Hence complex conjugation on the conjugate pairs of roots of f gives an order 2 element of G. In particular, $G \ncong Z/5Z$ and thus $G \cong D_{10}$.

13 August 2012

1: By Sylow's Theorem, there are either 1 or 6 Sylow 5-subgroups. If G is simple, then there must be 6 Sylow 5-subgroups and G acts on the set of these groups by conjugation so that there is a homomorphism mapping G to S_6. Because G is simple, the kernal of this map must be trivial so that the map is injective. Also, a simple group cannot have a subgroup of index 2, so G can be considered a subgroup of A_6. By the Orbit-Stabilizer Theorem, $|G : N_G(H)| = n_5 = 6$ so that $|N_G(H)| = 20$ for any Sylow 5-sugroup H. S_6 acts on its order-5 subgroups by conjugation, so the Orbit Stabilizer yields $|N_{S_6}(H)| = \frac{|S_6|}{|Orb_{S_6}(H)|} = \frac{6!}{6 \cdot 43 \cdot 2} = 20$, where H is the subgroup of G as it appears in S_6 under the injective homomorphism. Thus, $|N_{A_6}(H)| = 10$. But 20 does not divide 10, contradicting $N_G(H) \leq N_{A_6}(H)$.

2: We will prove this using the following two theorems: (1) if there is a proper subgroup $H \lhd G$, then G is solvable if and only if H and G/H are solvable and (2) all p-groups are solvable. The only divisor of 2^3 that is 1 mod 13 is 1 so that, by Sylow's Theorem, any group G of order 104 has a normal subgroup N of order 13. Then $|G/N| = 8$ so that G/N is a p-grpup. Since every p-group is solvable and both H and G/H are p-groups, then G is solvable.

3(a): Let I be a prime ideal and pick any $ab \in I$ such that $a \notin I$. Then $b \in I$, proving that $b^m \in I$ for some power m so that I is primary.

(b): Let $ab \in I'$ and assume $a \notin I'$. Then for some power m, $(ab)^m \in I$ and since R is commutative, $a^m b^m \in I$. We know $a^m \notin I$ for any power m since $a \notin I'$, so there is some power n such that $(b^m)^n \in I$. Then $b^{mn} \in I$ so that $b \in I'$.

(c): Let I be a primary ideal and let b generate I. Assume there are two distinct irreducibles a_1 and a_2 that divide b and let $a_1^i a_2^j r \in (b)$ for some $r \in R$ where neither a_1 nor a_2 divide r. Then neither $(a_1^i r)^m$ nor $(a_2^j r)^m$ are in I since neither are divisible by both irreducibles. Thus, b can only be divisible by at most one irreducible, a, so that $b = a^m$ for some m. Then $(b) = (a)^m$.

4: Let J be the Jordan canonical form of B. Since B has distinct eigenvalues then the Jordan canonical form of B is a diagonal matrix. Write $J = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$

and let $A = (a_{ij}) \in \{A \in M_n(K) : AB = BA\}$. If B is in Jordan canonical form then, $(a_{ij}\lambda_j) = AB = BA = (\lambda_i a_{ij})$. Since $\lambda_i \neq \lambda_j$, $a_{ij} = 0$ for $i \neq j$. Thus A is diagonal.

If B is not in Jordan canonical form then B is a similar to its Jordan canonical form so $B = PJP^{-1}$ for some invertible matrix P. Then $APJP^{-1} = AB = BA = PJP^{-1}A$, implying $P^{-1}APJ = JP^{-1}AP$. Thus $P^{-1}AP$ commutes with J. By an analogous argument as above $P^{-1}AP$ is a diagonal matrix. Therefore,

$$\{A \in M_n(K) : AB = BA\} \cong \{A \in M_n(K) | A \text{ is diagonal}\} \cong \mathbb{F}^n$$

is an n-dimensional vector space over $\mathbb{F}$.

5:

6(a): The roots of $x^8 - 1$ are the roots of unity $\{e^{\frac{2\pi ik}{8}}\}_{k\in Z_8}$, which are all generated by the root $\omega = e^{\frac{2\pi i}{8}}$. Then an element of $Gal(Q(\omega)/Q)$ is defined by where it sends ω. To be injective, the automorphism must send ω to a root of the same order. The order-8 roots are $\omega, \omega^3, \omega^5$, and ω^7. $\phi(\omega) = \omega$ is the identity automorphism. If ϕ maps ω to any other root, it turns out that ϕ is order-2. The only order-4 group that has such structure is $Z_2 \times Z_2$, which is the same structure as $Z_8^\times$.

(b): Denote the two generators of $Gal(Q(\omega)/Q)$ as $\phi_a(\omega) = \omega^3$ and $\phi_b(\omega) = \omega^5$. Then the subgroups are $\{e, \phi_a\}$, and $\{e, \phi_b\}$,$\{e, \phi_a \circ \phi_b\}$. These correspond to the extensions $Q(\sqrt{2}i), Q(i)$, and $Q(\sqrt{2})$, respectively.

14 January 2013

1: Let $(b, h) \in A \rtimes H$. We have $(b, h)(a, 1) = (b(h\cdot a), h)$ and $(a, 1)(b, h) = (a(1\cdot b), h)$, so $(b, h) \in C_G(a)$ if and only if $b(h \cdot a) = a(1 \cdot b)$. Now, $1 \cdot b = b$ and, since A is abelian, $ab = ba$, so $(b, h) \in C_G(a)$ if and only if $h \cdot a = a$, i.e. $h \in C_H(a)$. Hence $|C_G(a) = |A| \cdot |C_H(a)|$, which gives the size of the conjugacy class of a in G is $\frac{|G|}{|C_G(a)|} = \frac{|A|\cdot|H|}{|A|\cdot|C_H(a)|} = |H :_H (a)|$.

2(a): Let $x \in HK$ such that $x^{-1}Px \cap H \in Syl_p(H)$. Then since $H \lhd HK$, $x(x^{-1}Px \cap H)x^{-1} = P \cap xHx^{-1} = P \cap H \leq H$. Now, $x^{-1}Px \cap H = P \cap H$, so $P \cap H \in Syl_p(H)$. Similarly, $P \cap K \in Syl_p(K)$.

Since $H, K \lhd HK$, $P \cap H \lhd P$ and $P \cap K \lhd P$, it follows that $(P \cap H)(P \cap K) \leq P$. Now p does not divide $|H : P \cap H|$ nor $|K : P \cap K|$ and $|HK : (P \cap H)(P \cap K)| = \frac{|H:P\cap H|\cdot|K:P\cap K|}{|H\cap K:(H\cap K)\cap P|}$ so that p does not divide $|HK : (P \cap H)(P \cap K)|$. Since $(P \cap H)(P \cap K)$ is a p-subgroup of HK, it follows that $(P \cap H)(P \cap K) \in Syl_p(HK)$ and $P = (P \cap H)(P \cap K)$.

2(b): Let $P \in Syl_p(HK)$ for some p dividing $|HK|$. Then by part a, $P = (P \cap H)(P \cap K)$ and $P \cap H \in Syl_p(H)$ and $P \cap K \in Syl_p(K)$. Since H and K are nilpotent, $P \cap H$ char $H \lhd HK$ and $P \cap K$ char $K \lhd HK$. Hence $P = (P \cap H)(P \cap K) \lhd HK$. Since the prime p and $P \in Syl_p(HK)$ were chosen arbitrarily, every Sylow subgroup of HK is normal and HK is nilpotent.

3: $(\frac{1}{2}x + 1)(x + 4) = \frac{1}{2}x^2 + 3x + 4 = (x + 2)(\frac{1}{2}x + 2)$. Although both of these factorizations are equal to $\frac{1}{2}(x+2)(x+4)$ in $Q[x]$, $\frac{1}{2}$ is not an element of the subring, so the factorizations in the subring are distinct.

4(a): The condition is equivalent to the condition that $f(A) = 0$, where $f(x) = x^4 - x^2 + 2$. First, we show that f is irreducible over Q. Consider $x^4 + 2x^2 + 2 \in Z/3Z[x]$. Since this polynomial has no roots in $Z/3Z$, it has no linear factors in $Z/3Z[x]$. Thus, either f is irreducible or has a factor of degree 2. The only irreducible polynomials of degree 2 over $Z/3Z[x]$ are $x^2 + 1$ and $x^2 + x + 2$. Since $(x^2 + 1)^2 = x^4 + x^2 + 1$ and $f(x) = (x^2 + x + 2)(x^2 + 2x + 1) + x$, f is irreducible in $Z/3Z[x]$, and thus also irreducible in $Z[x]$. Now irreducibility in $Q[x]$ follows by Gauss' Lemma.

Suppose that $f(A) = 0$ for some $A \in M_6(Q)$. Then $m_A(x)$ divides $f(x)$, where $m_A(x) \in Q[x]$ is the minimal polynomial for A. Thus, $m_A(x) = f(x)$, by the irreducibility of $f(x)$. Every invariant factor of A must divide $m_A(x)$ and since $m_A(x)$ is irreducible, it follows that $m_A(x)$ is the only invariant factor of A. However, the product of the invariant factors of A gives the characteristic polynomial of A, a polynomial of degree 6, a contradiction. Hence no such A exists.

4(b): Since the roots of $f(x) = x^4 - x^2 + 2$ are $\pm\sqrt{\frac{1}{2} \pm \frac{\sqrt{-7}}{2}}$, the polynomial $a(x) = \left(x - \sqrt{\frac{1}{2} + \frac{\sqrt{-7}}{2}}\right)\left(x - \sqrt{\frac{1}{2} - \frac{\sqrt{-7}}{2}}\right) = x^2 - \left(\sqrt{\frac{1}{2} + \frac{\sqrt{-7}}{2}} + \sqrt{\frac{1}{2} - \frac{\sqrt{-7}}{2}}\right)x + \sqrt{2} = x^2 - \sqrt{1 + 2\sqrt{2}}x + \sqrt{2}$ divides $f(x)$. Consider the matrix $A = \begin{pmatrix} \mathcal{C}_{a(x)} & 0 \\ 0 & \mathcal{C}_{f(x)} \end{pmatrix} =$

$\begin{pmatrix} 0 & -\sqrt{2} & 0 & 0 & 0 & 0 \\ 1 & \sqrt{1+2\sqrt{2}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$. Since $a(x)$ divides $f(x)$, A is in rational canonical form. Furthermore, we see from the rational canonical form that the minimal polynomial of A is $m_A(x) = x^4 - x^2 + 2$, so A satisfies $A^4 - A^2 + 2I = 0$, whence $A^4 + I = A^2 - I$.

5: If a root of 2013^{th} lies in F_{67}, then it is also a 66^{th} root of unity and its order must then divide $(2013, 66) = 33$. Furthermore, F_{67} contains all the 33^{rd} roots of unity since 33 divides 66. Thus, there are 33 roots of $x^{2013} - 1$ in F_{67}.

6: Since E/F is normal, E/F is Galois. Furthermore, $[E : F] = p$, so $Gal(E/F)$ is cyclic. Hence E/F is a cyclic extension. Now, F contains all the p^2th roots of unity, therefore F must contain all p^{th} roots of unity, whence $E = F\left[\sqrt[p]{a}\right]$ for some $a \in F$ (see Dummit and Foote Proposition 14.37). Observe that F does not contain $\sqrt[p^2]{a}$, for it it did, F would also contain $\sqrt[p]{a}$, which is not the case. Consider the polynomial $f(x) = x^{p^2} - a \in F[x]$. The roots of this polynomial are $(\zeta_{p^2}^i)\sqrt[p^2]{a}$, for $0 \leq i \leq p^2 - 1$, where ζ_{p^2} is a primitive p^2th root of unity. Since $\zeta_{p^2} \in F$, if F were to contain a root of $f(x)$, $f(x)$ would split in F. Hence this is not the case and $f(x)$ is irreducible over F. (Only proves no linear factors?) From this it follows that $[K : F] = p^2$, where $K = F\left[\sqrt[p^2]{a}\right]$. Now, $\sqrt[p]{a} = (\sqrt[p^2]{a})^p \in K$, so $E \subset K$ and K is an extension of E. Moreover $[K : E] = \frac{[K:F]}{[E:F]} = p$.

15 August 2013

1(a): Let $H < G$ such that $[G : H] = p$ and note that G acts on the cosets of H by left multiplication. Then there is a homomorphism $\phi : G \to S_p$. Because the only elements that fix the identity coset are elements of H, then $ker(\phi) < H$. If $ker(\phi) = 1$, then G is isomorphic to a subgroup of S_p so that $G = Z_p$, forcing H to be the normal trivial subgroup. Let $ker(\phi)$ be nontrivial. Because $G/ker(\phi) \cong im(G) < S_p$, then p divides $|im(G)|$ and $|im(G)|$ divides $p!$ so that $|im(G)| = p$. Thus, $|G : ker(\phi)| = p$ so that $H = ker(\phi)$ which is then normal.

1(b): Because H and K are normal, then $H \cap K$ is a normal subgroup of H and K.

If $H \cap K$ is nontrivial, then because H and K are simple, $H = H \cap K = K$; a contradiction. Then $|HK : H| = |HK : K| = p$ where $H \cong K \cong Z_p$. Since $HK < G$, then $p = |G : H| = |G : HK||HK : H| = |G : HK|p$ and thus $G = HK = Z_p \times Z_p$.

2(a): For any $B \in GL_m(Z/p^mZ)$, $det(B)$ cannot divide p^m. Then it also cannot divide p^{m+1} so that $B \in GL_m(Z/p^{m+1}Z)$.

2(b): Let $\alpha p^m + \beta \in Z/p^{m+1}Z$ with $\alpha \in Z/pZ$ and $\beta \in Z/p^mZ$. Then the reduction map $\phi : Z/p^{n+1}Z \to Z/p^nZ$ is defined by $\phi(\alpha p^m + \beta) = \beta$. The kernal of this map are all matrices in $GL_m(Z/p^{m+1}Z)$ that have $\beta = 1$ for the diagonal entries and $\beta = 0$ for the remaining entries. Let $C = AB$ for some pair of elements $A, B \in GL_m(Z/p^{m+1}Z)$. Then we can calculate the entries as follows: $c_{ij} = \sum_{n=1}^{m} a_{in}b_{nj}$. Note that if both a_{in} or b_{nj} have zero βs, then we get a multiple of p^{m+1} and thus zero. For $i \neq j$, the only terms of the sum for c_{ij} that are nonzero are those that include diagonal entries from A or B: $c_{ij} = a_{ii}b_{ij} + a_{ij}b_{jj}$. Let $a_{ii} = \alpha_{a_i}p^m + 1, a_{ij} = \alpha_{a_j}p^m, b_{ij} = \alpha_{b_i}p^m$, and $b_{jj} = \alpha_{b_j}p^m + 1$. Then $c_{ij} = (\alpha_{a_i}p^m + 1)(\alpha_{b_i}p^m) + (\alpha_{a_j}p^m)(\alpha_{b_j}p^m + 1) = (\alpha_{b_i} + \alpha_{a_j})p^m$ for $i \neq j$. And $c_{ii} = (\alpha_{a_i}p^m + 1)(\alpha_{b_i}p^m + 1) = (\alpha_{a_i} + \alpha_{b_i})p^m + 1$ for $i = j$. Because $\alpha \in Z/pZ$, then the kernal is isomorphic to the additive group $M_m(Z/pZ)$.

2(c): We can calculate the order by counting the possible entries for each row. The first row can take on any combination of values from Z/pZ except all zeroes: $p^m - 1$. The next row can't be a multiple of the first: $p^m - p$. Generally, the i^{th} row cannot be a linear combination of the previous $i - 1$ rows: $p^m - p^{i-1}$. Then we get an order of $\prod_{i=0}^{m-1}(p^m - p^i)$.

2(d): We can calculate the order of $GL_m(Z/p^mZ)$ using the above results: $|GL_m(Z/p^nZ)| = |GL_m(Z/p^{n-1}Z||M_m(Z/pZ)|$. Noting that $|M_m(Z/pZ)| = p^{m^2}$, we can inductively find that $|GL_m(Z/p^nZ)| = (p^{m^2})^{n-1}\prod_{i=0}^{m-1}(p^m - p^i)$.

3: Assume to the contrary that $M \neq \{0\}$ and let n be the smallest integer such that M is generated by n elements, say $m_1, \ldots, m_n$. Since $PM = M$ we have $m_n = p_1m_1 + p_2m_2 + \ldots + p_nm_n$ for some $p_1, p_2, \ldots, p_n \in P$. Thus $(1 - p_n)m_n = p_1m_1 + \ldots + p_{n-1}m_{n-1}$. We claim $1 - p_n$ is a unit. If $1 - p_n$ is not a unit then it must be contained in P as P is a unique maximal ideal. This implies $1 - p_n = p$ for some $p \in P$. Then $1 = p + p_n \in P$, which is a contradiction. Hence $1 - p_n$ is a unit so m_n lies in the module generated by $m_1, \ldots, m_{n-1}$ contradicting the minimality of n. Therefore $M = \{0\}$.

To see that the hypothesis that M be finitely generated is necessary consider $A = \mathbb{Q}[x]$, $P = x\ \mathbb{Q}[x]$, and $M = \mathbb{Q}[x, x^{-1}]$. Since P is the only ideal of A such that $A/P \cong \mathbb{Q}$, which is a field, then P is a unique maximal ideal. Next we claim M is infinitely generated. This is because if S is a finite generating set of M then there exists a minimal j such that x^j is assumed at some polynomial in S. But then $x^{j-1} \notin AS$ contradicting that $M = AS$. Hence M is infinitely generated. Furthermore $PM = M$, thus the hypothesis that M be finitely generated is indeed necessary.

4: Because k is algebraically closed, $M = PJP^{-1}$ for some matrix J that is in Jordan canonical form. Define S_J to be the diagonal matrix with the eigenvalues of J down the diagonal. Let $U_J = JS_J^{-1}$ so that $U_J S_J = J$ and the eigenvalues of U_J are all 1. Because J is upper-triangular, then so is U_J and thus $U_J S_J = S_J U_J$. Then conjugating everything by P yields: $PS_JP^{-1}PU_JP^{-1} = PU_JP^{-1}PS_JP^{-1} = PJP^{-1} = M$. Thus, we get a diagonalizable $S = PS_JP^{-1}$ and a matrix with all eigenvalues equal to 1 $U = PU_JP^{-1}$ such that $US = SU = M$.

5: Since $F \subset D \subset E$ then D is a commutative ring with identity so it suffices to show every nonzero element of D has an inverse. Let d be a nonzero element of D. Since $[E : F]$ is finite then E is algebraic over F. Thus $d \in D \subset E$ is the root of some polynomial $p(x) \in F[x]$ so there exist elements $a_i \in F$ such that $d^n + a_{n-1}d^{n-1} + \ldots + a_1 d + a_0 = 0$. Then, $1 = -a_0^{-1}(d^{n-1} + a_{n-1}d^{n-1} + \ldots + a_1)d$. Thus, $-a_0^{-1}(d^{n-1} + a_{n-1}d^{n-1} + \ldots + a_1) \in D$ is the inverse of d. Hence D is a field.

If $[E : F]$ is infinite consider $F = \mathbb{Q}$ and $E = \mathbb{Q}(x)$, the field of fractions of $\mathbb{Q}$. Then $D = \mathbb{Q}[x]$ is a intermediate subring that is not a field.

6(a): A theorem gives that numbers are constructible from a base field iff the extension is a power of 2. There are 16 primitive 17^{th} roots of unity so that a field extension adjoining one of these roots is a degree-16 extension. Therefore, the 17-gon is constructible.

(b): Similarly, there are 18 primitive 19^{th} roots of unity giving a degree-18 extension. Since this is not a power of 2, then the 19-gon is not constructible.

16 January 2014

1(a): Let $|G:H| = k$ and $\phi : G \to S_k$ be the homomorphism defined by how elements of G permute the cosets of H. Then $ker(\phi) \subset H$, since only elements of H will stabilize the identity coset H, and $ker(\phi)$ is normal. By the first Isomorphism Theorem, $G/ker(\phi) = im(G) \subset S_k$.

(b): Let $\phi : G \to S_5$ be the homomorphism defined by how elements of G permute the cosets of the given order-2 subgroup. Because the subgroup is not normal and must contain $ker(\phi)$, then $ker(\phi) = 1$ so that $G \cong \phi(G) \subset S_5$.

2. First note that $143 = 11 \cdot 13$. By Sylow's theorem, the number of Sylow-11 subgroups divides 13 and is $1(mod\ 11)$. Then there is only 1 Sylow-11 subgroup that must then be normal. Similarly, there is only one Sylow-13 subgroup that must be normal. Because these groups of relatively prime orders must have trivial intersections, then the group is isomorphic to the direct product of these two normal subgroups. And the directo product of relatively prime groups yields a cyclic group.

3. True. Let $r \in R$ have no multiplicative inverse and consider the ideal $(r, x) \subset R[x]$. If $(r, x) = (f)$ for some $f \in R[x]$, then f divides both r and x. The former forces $f \in R$. But now the latter is impossible since the coefficient of x is a unit and r is not.

4: Consider $(x, y) \in R^2$ with $x \neq 0$ and $y \neq 0$. Then, $T(x, y) = (0, y)$ gives us elements in the ideal $((x, y))$ that span R^2 so that the ideal is all of R^2. Clearly, $T(0, 0) = r(0, 0) = (0, 0)$ so that $(0, 0)$ generates the trivial ideal. Consider $(x, 0)$ with $x \neq 0$. Then $T(x, 0) = (0, 0)$ and $r(x, 0) = (rx, 0)$ for every $r \in R$ so that $(x, 0)$ generates $x-axis$ as an ideal. Finally, $T(0, y) = (0, y)$ and $r(0, y) = (0, ry)$ demonstrates that $(0, y)$ with $y \neq 0$ generates the y-axis as an ideal.

5(a): Let $X = \{E \supset F :$ -1 is not a sum of finitely many squares in $E\}$. Then X is partially ordered by inclusion. Assume that -1 is the sum of finitely many squares in $\cup X$: $-1 = x_1^2 + ... + x_n^2$. I want to say there must be a single E that contains these squares, giving a contradiction, but why must there be such an E?

5(b): Let $a = g_1^2 + ... + g_k^2$ with $g_1, ..., g_k \in G$ and assume $\sqrt{a} \notin G$. Then $G[\sqrt{a}]$ is a proper field extension of G so that $-1 = (i_1 + \sqrt{a}j_1)^2 + ... + (i_k + \sqrt{a}j_n)^2$ for some finite n elements from $G[\sqrt{a}]$. Multiplying these terms out yields $-1 = (i_1^2 + ... + i_n^2) + a(j_1^2 + ... + j_n^2) + 2\sqrt{2}(i_1 j_1 + ... + i_n j_n)$. Since -1 has no multiples of $\sqrt{a}$, then the final part of the sum must be zero. Since a is a sum of squares in G and $i_1^2, ..., i_n^2, j_1^2, ..., j_n^2$ are all squares in G, then we get that -1 is a finite sum of squares in G; a contradiction. Thus, $\sqrt{a} \in G$.

6(a): Trivially, $a \sim a$ and $a \sim b \Rightarrow b \sim a$. If $(a,b),(b,c) \in G$, then $(a,b)(b,c)(a,b) = (a,c) \in G$. Consider it noted that G acts on I. Now let $A = \{a_1, ..., a_n\}$ and B be non-empty equivalence classes. Let $\sigma \in G$ be such that $\sigma(a_1) \in B$. Then for every $(a_1, a_i) \in G$, we get $\sigma(a_1, a_i)\sigma^{-1} = (\sigma(a_1), \sigma(a_i)) \in G$ so that $|B| = |A|$.

6(b): Because $f(x)$ has two imaginary roots, then one of the elements of the automorphism group is the transposition of these two imaginary roots. Then using the equivalence relation above, the equivalence class containing these roots has a size of at least two. Since the automorphism group acts transitively on the roots, then each equivalence class must be the same size so that the size of one class must divide the number of roots. Since there are a prime number of roots and we've found a class that has more than one element, then there must only be one equivalnce class. Thus, the group contains every transposition; namely, the group is S_p.

17 August 2014

1: Since the conjugacy class of a inside G is of size m, this is equivalent to saying $|G : C_G(a)| = m$. Notice that the size of the conjugacy class of a inside H is $|H : C_H(a)|$ where $C_H(a) = C_G(a) \cap H$. If $C_G(a) \subseteq H$, then $C_H(a) = C_G(a)$ so $|H : C_H(a)| = |G : C_G(a)|/|G : H| = m/p$. If $C_G(a) \nsubseteq H$, then there exists some element $b \in C_G(a) \backslash H$. The subgroup $\langle H, b\rangle$ must be G since the index of H is prime, and therefore the only group that properly contains H is G. Thus $HC_G(a) = G$ and the second (diamond) isomorphism theorem gives

$$\frac{|G|}{|H|} = \frac{|C_G(a)|}{|C_H(a)|} \quad \longrightarrow \quad \frac{|G|}{|C_G(a)|} = \frac{|H|}{|C_H(a)|} = m$$

2: Let n_p be the number of Sylow p-subgroup for prime p. By Sylow's Theorem, $n_{11} \mid 23$ and $n_{11} \equiv 1 \mod 11$, so $n_{11} \in \{1, 23\}$. By the same part of Sylow's theorem, $n_{23} = 1$. Let H be a Sylow 11-subgroup and K be the unique Sylow 23-subgroup. The orders of H and K are prime, so they are isomorphic to $\mathbb{Z}/11\mathbb{Z}$ and $\mathbb{Z}/23\mathbb{Z}$, respectively. Since $H \cap K = \{1\}$, K is normal in HK, and $|H||K| = |HK|$, we know that G

is isomorphic to $H \ltimes_\phi K$ for some appropriate homomorphism $\phi : \mathbb{Z}/11\mathbb{Z} \to (\mathbb{Z}/23\mathbb{Z})$.

$(\mathbb{Z}/23\mathbb{Z}) \cong \mathbb{Z}/22\mathbb{Z}$, so we seek homomorphisms $\phi : \mathbb{Z}/11\mathbb{Z} \to \mathbb{Z}/22\mathbb{Z}$. The kernel of this homomorphism is a subgroup of $\mathbb{Z}/11\mathbb{Z}$, so $\ker\phi = \mathbb{Z}/11\mathbb{Z}$ or is trivial. If $\ker\phi = \mathbb{Z}/11\mathbb{Z}$, then the homomorphism is the trivial homomorphism and the semidirect product defined by this homomorphism is in fact the direct product. If $\ker\phi$ is trivial, then the map is injective, so $\mathbb{Z}/11\mathbb{Z}$ is isomorphic to a subgroup of $\mathbb{Z}/22\mathbb{Z}$. There is only one such subgroup, namely, $\langle 2\rangle$. By the theorem that states that two homomorphisms from a cyclic group with the same image form isomorphic semidirect products, we know that all the possible homomorphisms from $\mathbb{Z}/11\mathbb{Z}$ to $\langle 2\rangle$ produce isomorphic semidirect products. Thus there are 2 groups of order 253: The direct product $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ and the semidirect product $\mathbb{Z}/11\mathbb{Z} \ltimes_\phi \mathbb{Z}/23\mathbb{Z}$.

3(a): Take any element in IJ. Then this element is of the form $i_1j_1 + i_2j_2 + \cdots + i_nj_n$ where all $i_k \in I$ and $j_k \in J$. By the absorption property of ideals, each i_kj_k is in I and in J, and thus is in $I \cap J$. By closure of ideals under addition, the entire sum of $i_kj_k \in I \cap J$. Thus the left-hand side is contained in the right-hand side.

I, J are comaximal, so there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Let $a \in I \cap J$. Then $a = a \cdot 1 = a \cdot (i + j) = ai + aj$. By the absorption property of ideals, each summand is in IJ and by closure under addition the sum is in IJ. Thus $a \in IJ$.

3(b): Let $R = \mathbb{Z}$, $I = (2)$ and $J = (4)$. I, J are not comaximal. $I \cap J = J = (4)$, but $IJ = (8)$.

4(a): $A^3 = -A$ is equivalent to saying A is annihilated by the polynomial $f(x) = x^3 + x$. This means the minimal polynomial $m_A(x)$ divides $f(x)$. Since $f(x)$ has no repeated roots and all of its distinct roots exist in , then its Jordan canonical form is a diagonal matrix. And since every matrix is similar to its Jordan canonical form, then A is diagonolizable.

4(b): The characteristic polynomial of A is of degree 2, so its minimal polynomial is of degree 1 or 2. From part (a), we know that $m_A(x) = x^1 + 1$, x, or x^2. Since A has no non-trivial eigenvectors, it cannot have zero eigenvalues, so the minimal polynomial cannot be x or x^2. We use $m_A(x) = x^2 + 1$ to obtain the rational canonical form of A, which is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Every matrix is similar to its rational canonical form, so the proof is complete.

5: Recall that $x^{p^n} - x$ is equal to the product of all irreducible polynomials of degree d for every d dividing n. Thus $x^{3^6} - x$ is the product of all degree 1, 2, 3, and 6 irreducible polynomials over $_3$. The list of irreducibles of degree 1 is $\{x, x+1, x+2\}$. The irreducibles of degree 2 are the factors of $\dfrac{x^{3^2} - x}{x(x+1)(x+2)}$, so by degree considerations, there are 3 of them. The irreducibles of degree 3 are the factors of $\dfrac{x^{3^3} - x}{x(x+1)(x+2)}$, so there are 8 of them. Finally the irreducibles of degree 6 are the factors of the quotient of $x^{3^6} - x$ by the product of all irreducibles of degree 1, 2, and 3. By degree considerations, there are $\dfrac{3^5 - 11}{2}$ of them.

6(a): $\alpha^2 - 4 = 3\sqrt(2) \rightarrow \alpha^4 - 8\alpha^2 + 16 = 18$, so α is a root of $f(x) = x^4 - 8x^2 - 2$. This polynomial is irreducible by Eisenstein's criterion, so it is the minimal polynomial for α.

6(b): Let $\beta = \sqrt{4 - 3\sqrt{2}}$. Notice that β is also a root of $f(x)$. Since α is formed by only taking square roots of positive numbers, we know $(\alpha) \subseteq$. If (α) is Galois, then any irreducible polynomial with one root in the field should split in the field. In particular, β should be in (α). This implies that $\alpha\beta \in (\alpha)$. But $\alpha\beta = \sqrt{-2} \notin$. Thus $\beta \notin (\alpha)$ and (α) is not Galois.

6(c): The degree of a simple extension is the degree of the minimal polynomial of the element used to form the extension, so $[(\alpha)/] = 4$. Notice that β is a root of $x^2 - (8 - \alpha^2) \in (\alpha)[x]$. This must be the minimal polynomial of β over (α) since the Galois closure of (α) must be a proper extension. Thus $M = (\alpha, \beta)$ is the Galois closure and it is an extension over of degree $4 \cdot 2 = 8$. By the fundamental theorem of Galois theory, the order of the Galois group of $M/$ is 8.

18 January 2015

1(a): False. Let G be the free product of cyclic groups H and K. Then $HK = \{h^i k^j | i, j \in Z\}$ and $KH = \{k^i h^j | i, j \in Z\}$. But hkh is not equal to any of the elements in HK nor KH since there are no relations on G. Then neither HK nor KH is closed under the operation on G.

(b): True. Order the finitely many elements in G and define the homomorphism

$\phi : G \to GL_n(C)$ which sends an element in G to a matrix describing how that element permutes the other elements under left multiplication. Because each element in G permutes the other elements in a unique way, this is an injective map and thus an isomorphism to a subgroup of $GL_n(C)$. Maybe need to write down the matrix entries explicitly?

2(a): Sylow's theorem states that G acts transitively on the set of Sylow subgroups by conjugation. So, G conjugates each of the Sylow p-subgroups into each other. Since $U \triangleleft G$, then G conjugates U back to itself so that if any of the Sylow p-subgroups are subgroups of U, then all of them are.

(b): If H acts transitively on $Syl_p(U)$, then by the orbit-stabilizer theorem, $|H| = |Syl_p(Q)| \cdot |Stab_H(Q)|$ for each $Q \in Syl_p(U)$. Then the number of Sylow p-subgroups in U divides the order of H. But this number must also divide the order of U and since these orders are relatively prime, then $|Syl_p(U) = 1|$ so that Q is normal in U. Now let there be a Sylow p-sugroup $Q \triangleleft U$. Since we are given that $Syl_p(U) \cap Syl_p(G) \neq 0$, then by part a, $Q \triangleleft G$. Since every element of G conjugates Q to itself, H acts transitively on this singleton set.

3(a): The units of R are the fractions that, in reduced form, have odd numerators. Then every element can be written as $2^k u$ for some non-negative integer k and a unit u. If $k > 1$, then $2^k u = 2 \cdot 2^{k-1} u$. Since 2 and $2^{k-1}u$ have even numerators, they are not units so that r is reducible. Thus, r is irreducible only if it has a single power of 2 in the numerator. Part b proves that R is a Euclidean Domain so that primes and irreducibles are the same.

3(b): Define a norm $v : R \setminus 0 \to Z$ by $v(2^k u) = k$. Pick any $2^n u, 2^m v \in R$ and assume WLOG that $m \leq n$. Then $\frac{2^n u}{2^m v} = 2^{n-m} \frac{u}{v} \in R$, since $\frac{u}{v}$ is a unit. Thus, every pair of elements has the property that one element divides the other and therefore the remainder from the Euclidean algorithm is always zero, certainly satisfying the requirement that the remainder have a smaller norm than the element being divided.

4: Consider the polynomial $(x+1)(x-(n-1))$. Plugging in $J-I$ yields $J(J-nI) = 0$. The minimum polynomial cannot be linear since $J - I$ is not a scalar multiple of I. Then $(x+1)(x-(n-1))$ is the minimum polynomial of $J - I$, giving us eigenvalues of -1 and $n-1$. Let v be in the eigenspace of $n-1$; namely, $(J-I)v = (n-1)v$. Then consider hte i^{th} row of this equivalence: $v_1 + \ldots + v_{i-1} + v_{i+1} + \ldots + v_n = (n-1)v_i$. Adding v_i to both sides demonstrates that nv_i is the sum of all entries of v. SInce we chose arbitrarily, all entries of v must be equal so that the eigenspace of $n-1$ has dimension 1. Then only one of the invariant factors of $J-I$ is divisible by $(x-(n-1))$ so that the characteristic polynomial of A is $(x+1)^{n-1}(x-(n-1))$. Then the Jordan canonical form of $J-I$ has: (1) an $(n-1)\times(n-1)$ with 1's along the first super-diagonal and -1's downt he diagonal and (2) a 1×1 block with $(n-1)$ as its sole entry. The determinant of this matrix is $(n-1)\neq 0$ so that $J-I$ is invertible.

5(a): $F_p(t)$ is the field of fractions of the UFD $F_p[t]]$ so that, by Gauss's Lemma, x^p-t is irreducible over $F_p(t)$ if it is irreducible over $F_p[t]$. Assume that $x^p-t = g(x,t)h(x,t)$ for some elements of $F_p[x,t]$. Because there is only one power of t, then either $g(x,t)$ or $h(x,t)$ is in $F_p[x]$. WLOG, let $(f(x))^p - t = g(x)h(x,t)$. Then $h(x,t)$ has a single power of t that multiplies by the terms in $g(x)$ to yield only t. Then $g(x)$ must be a unit, so that x^p-t is irreducible. Am I missing any details?

(b): The degree of $[F(\alpha):F]$ equals the degree of the minimum polynomial of α; namely, p. Since Z/pZ is the only group of order p, it is the automorphism group of the extensions $F[\alpha]/F$.

6(a): Let f be the degree-4 separable polynomial and α a root. Then $|F[\alpha]:F| = 4$ so that $|K:F[\alpha]| = 2$. Then f must factor over $F[\alpha]$ into two linear factors and a quadratic factor. So, $F[\alpha]$ contains two roots of f. Let β be a zero of the quadratic factor so that $F[\alpha]\neq F[\beta]$. Similarly, $F[\beta]$ contains the other two roots, giving us precisely two extensions such that $|K:F[\alpha]| = |K:F[\beta| = 2$. Then $Gal(K/F)$, which has order 8, has precisely two subgroups of order 2. There are five groups of order 8 up to isomorphism: $Z/8Z$, $Z/4Z\times Z/2Z$, $Z/2Z\times Z/2Z\times Z/2Z$, D_8, and Q_8. Only $Z/4Z\times Z/2Z$ has precisely two subgroups of order 2.

(b): There's one order 4 subgroup of $Z/4Z\times Z/2Z$, so there can only be one subextension of order 2.