Algebra Prelim Solutions, Spring 1980

1. We shall use the fundamental theorem for finitely generated abelian groups. We may write

$$A = \bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})^{a_i}, \quad B = \bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})^{b_i}, \quad C = \bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})^{c_i}$$

where a_i, b_i, c_i, n are nonnegative integers, and the q_i are distinct prime powers. Then $A \oplus B \cong A \oplus C$ yields

$$\bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})^{a_i+b_i} \cong \bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})^{a_i+c_i}$$

The fundamental theorem now shows that $a_i + b_i = a_i + c_i$ and hence $b_i = c_i$ for all i. It follows that $B \cong C$ as required.

2. Suppose by way of contradiction G is a simple group of order 56. Sylow's theorem for the prime 7 shows that the number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 8, hence the number of Sylow 7-subgroups is 1 or 8. If there is one Sylow 7-subgroup, x then this subgroup must be normal in G which contradicts the hypothesis that G is simple, consequently G has 8 Sylow 7-subgroups.

   Let A, B be two distinct Sylow 7-subgroups. Then $A \cap B$ is a subgroup of A, so by Lagrange's theorem $|A \cap B|$ divides $|A|$, hence $|A \cap B| = 1$ or 7. Now A and B both have order 7, so we cannot have $|A \cap B| = 7$. Therefore we must have $|A \cap B| = 1$. Since every nonidentity element of a Sylow 7-subgroup has order 7, we deduce that G has at least 6×8 elements of order 7.

   Now every Sylow 2-subgroup has order 8, and every element of a Sylow 2-subgroup has order a power of 2 by Lagrange's theorem, so if G has at least two Sylow 2-subgroups, then G has at least 9 elements of order a power of 2. Since we have already shown that G has at least 48 elements of order 7, we now have that G has at least $9 + 48 = 57$ elements, which is not possible because $|G| = 56$. Therefore G has exactly one Sylow 2-subgroup, and so this Sylow subgroup must be normal which contradicts the hypothesis that G is simple.

3. Since we are working over $\mathbb{C}$, an algebraically closed field, we may use the Jordan canonical form. Here every matrix has a unique Jordan canonical form, and two canonical forms are in the same equivalence class of T

if and only if they are equal. Since the eigenvalues of a matrix in T are 4,4,17,17,17, the Jordan canonical form of such a matrix must look like

$$\begin{pmatrix} 4 & a & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 17 & b & 0 \\ 0 & 0 & 0 & 17 & c \\ 0 & 0 & 0 & 0 & 17 \end{pmatrix}$$

where a,b,c are 1 or 0, and $b = 0$ if $c = 0$. Therefore there are $\boxed{6}$ equivalence classes in T.

4. There are many answers to this problem; perhaps the simplest example of a UFD which is not a PID is $\mathbb{Z}[X]$. This is a UFD because $\mathbb{Z}$ is a UFD, and a polynomial ring over UFD is again a UFD. We now establish that $\mathbb{Z}[X]$ is not a PID by showing that the ideal $(2,X)$ (the ideal generated by 2 and X) is not principal.

   Suppose on the contrary that $(2,X) = f$ for some $f \in \mathbb{Z}[X]$. Then there exist $g,h \in \mathbb{Z}[X]$ such that $fg = 2$ and $fh = X$. The equation $fg = 2$ shows that f must have degree 0, in other words $f \in \mathbb{Z}$, and then $fh = X$ shows that $f = \pm 1$. Thus we must have $(2,X) = \mathbb{Z}[X]$. Now the general element of $(2,X)$ is $2a + Xb$ where $a,b \in \mathbb{Z}[X]$. The constant term of $2a$ must be divisible by 2, and the constant term of Xb must be zero, hence the constant term of $2a + Xb$ must be divisible by 2. In particular we cannot have $2a + Xb = 1$, so $1 \notin (2,X)$ and we have the required contradiction.

5. Let G denote the Galois group of $x^3 - 10$ over $\mathbb{Q}$. By Eisenstein's criterion for the prime 2 (or otherwise), we see that $x^3 - 10$ is irreducible over $\mathbb{Q}$, hence $G \cong S_3$ or A_3. Let $\omega = (-1 + i\sqrt{3})/2$, a primitive cube root of unity. Then the roots of $x^3 - 10$ are $\sqrt[3]{10}$, $\omega\sqrt[3]{10}$, and $\bar{\omega}\sqrt[3]{10}$ ($\bar{\omega} = (-1 - i\sqrt{3})/2$), hence $x^3 - 10$ has one real root and two complex roots, so complex conjugation is an element of G. Therefore G has an element of order 2, which rules out the possibility $G \cong A_3$. Therefore $G \cong S_3$.

   A splitting field of $x^3 - 10$ is $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{10})$. The normal subfields of the splitting field correspond to normal subgroups of G. The normal subfields corresponding to the subgroups 1 and G are $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{10})$ and $\mathbb{Q}$ respectively. G has exactly one other normal subgroup, namely A_3, so there is exactly one other normal subfield. Since subfields of degree two over $\mathbb{Q}$ are always normal, this other normal subfield must be $\mathbb{Q}(i\sqrt{3})$.

6. (a) How to prove this depends on how much field theory one is allowed to assume. Also the result is true without the hypothesis that f is separable. Here is one way to proceed. Suppose K_1, K_2 are fields, $\theta\colon K_1 \to K_2$ is an isomorphism, $g \in K_1[X]$ is an irreducible polynomial, α_1 is a root of g in a splitting field L_1 for g, and α_2 is a root of the irreducible polynomial θg in a splitting field L_2 for θg (recall if $g = a_0 + a_1X + \cdots + a_nX^n$ with $a_i \in K_1$, then $\theta g = \theta a_0 + \theta a_1 X + \cdots + \theta a_n X^n \in K_2[X]$). Then θ extends to an isomorphism $\phi\colon K_1(\alpha_1) \to K_2(\alpha_2)$ such that $\phi(\alpha_1) = \phi(\alpha_2)$. Using induction on the degree of g, we deduce that ϕ in turn extends to an isomorphism of L_1 onto L_2. This is what is required.

   (b) Note that $x^4 - 2$ is indeed irreducible over $\mathbb{Q}$, by Eisenstein's criterion for the prime 2. The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Consider the permutation of the roots $\sqrt[4]{2} \to \sqrt[4]{2}$, $-\sqrt[4]{2} \to i\sqrt[4]{2} \to -i\sqrt[4]{2} \to -\sqrt[4]{2}$. This cannot be induced by an element θ of the Galois group of $x^4 - 2$ over $\mathbb{Q}$, because if $\theta\sqrt[4]{2} = \sqrt[4]{2}$, then we must have $\theta(-\sqrt[4]{2}) = -\sqrt[4]{2}$.

7. Since $\mathrm{Hom}_A(M,k) = 0$, we must have $M = \mathscr{M}M$. Then Nakayama's lemma yields the result.

Spring 1993 Algebra Prelim Solutions

1. We use the structure theorem for finitely generated modules over a PID. This tells us that M is a direct sum of modules of the form R/Rt where t is either zero or a power of an irreducible element of R. If this direct sum has more than one factor, then we may write $M = A \oplus B$ for some nonzero submodules A, B of M, and then $A \cap B = 0$. Therefore there is exactly one factor in the direct sum, and the result follows.

2. (a) Since the action is transitive, all the stabilizers are conjugate and we see that the stabilizer of any element of X has no element of finite order other than 1. Thus if $f \in G$ has finite order larger than 1, then f cannot be in the stabilizer of any element of X, and it follows that f cannot fix any element of X.

   (b) Suppose now that f has prime order q. Then the orbits of f have order dividing q. Since q is prime, these orbits have order 1 or q. But if one of the orbits has order 1, then f fixes the element in that orbit which contradicts the above. Therefore all orbits of f have order q, and it follows that q divides $|X|$ as required.

3. Since $S/(P_1 \cdots P_t)$ is finite, we see that S/P_i is finite for all i. Now S/P_i is an integral domain because P_i is prime, and finite integral domains are fields. Therefore S/P_i is a field and we deduce that P_i is a maximal ideal for all i, as required.

4. Suppose K is a nontrivial extension field of F with degree which is not a power of p. Note that if L is any finite extension field of K, then the degree of L over F is also not a power of p, because $[L:F] = [L:K][K:F]$. Since we are in characteristic zero, everything is separable so by taking a splitting field containing K, we may assume that K is a Galois extension of F. Let $G = \mathrm{Gal}(K/F)$ and let P be a Sylow p-subgroup of G. Then $[K^P:F] = |G:P|$ and $[K:F] = |G|$. Since $|G:P|$ has order prime to p, it follows that $[K^P:F]$ has order prime to p and we conclude that K^P is a nontrivial extension field of F with degree prime to p.

5. This question depends on what we are allowed to assume; some people take the given property as the definition of projective module. Also the question does not require that R be commutative. Let us use the definition that an R module P is projective if and only if it is a direct summand of a free R-module. Suppose first that we have the given property. Choose an epimorphism $f: F \to M$ where F is a free R-module. Since the map $f_* : \mathrm{Hom}(M,F) \to \mathrm{Hom}(M,M)$ is surjective, there exists an R-module map $g: M \to F$ such that fg is the identity map on M. Then g is a monomorphism and so $M \cong gM$. Also $F = \ker f \oplus gM$, which shows that gM and hence also M are projective.

   Conversely suppose M is a direct summand of a free module F. First we show that F satisfies the given condition. Let $f: N \to N$ be a surjection of R-modules and let $h: F \to N$ be any R-map. Let $\{e_i : i \in I\}$ be an R-basis for F, where I is some indexing set. Since h is surjective, we may choose $n_i \in N$ such that $f(n_i) = h(e_i)$ for all i. Now we can define $g \in \mathrm{Hom}_R(F,N)$ by $g(e_i) = n_i$ for all i, and then $fg(e_i) = h(e_i)$ for all i. Thus $fg = h$, and we have proved the result in the case $M = F$.

   For the general case, write $F = M \oplus P$ as R-modules, and let $\psi: M \to F$ be the natural

monomorphism Then we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(F,N & \xrightarrow{f} & \mathrm{Hom}_R(F,N \\ \downarrow\psi & & \downarrow\psi \\ \mathrm{Hom}_R(M,N & \xrightarrow{f} & \mathrm{Hom}_R(M,N \end{array}$$

where $(\psi\ g\ (m \quad g(\psi m$ for all $m \quad M$ and $g \quad \mathrm{Hom}_R(F,N$ or $\mathrm{Hom}_R(F,N$. Note that the right hand (and also the left hand) ψ is surjective: if $h \quad \mathrm{Hom}_R(M,N$, we may extend h to an R-map $F \quad N$ by defining it to be 0 on P and then $\psi\ h \quad g$. By the previous paragraph the top f is surjective and we deduce that the bottom f is surjective as required.

6. The dihedral group has a cyclic subgroup C of index 2. Let χ denote the character of the regular representation of C. Since C is abelian, we may write $\chi \quad \alpha_1 \quad \cdots \quad \alpha_n$ for some integer n, where the α_i are degree one characters of C. Let ψ denote the character of V. Since χ^D is the character of the regular representation of D, we see that $\psi,\chi^D \quad 0$. Therefore $\psi,\alpha_i^D \quad 0$ for some i. Since ψ is irreducible, we deduce that $\alpha_i^D \quad \psi \quad \phi$ for some character ϕ of D. Therefore ψ has degree at most that of α_i^D. But α_i has degree 1, consequently α_i^D has degree 2 and the result follows.

7. Let G denote the Galois group of $X^{10}-1$ over $\mathbb{Q}$, and let ω be a primitive 10th root of 1 (so $\omega \quad e^{\pi i/5}$). Then the roots of $X^{10}-1$ are ω^r, where $r \quad 0,1,\ldots,9$, which shows that the splitting field for $X^{10}-1$ is $\mathbb{Q}\,\omega$. Since $X^{10}-1 \quad (X^5-1\ (X \quad 1\ (X^5 \quad 1\ /(X \quad 1$ and ω does not satisfy $(X^5-1\ (X \quad 1$, we see that ω is a root of $(X^5 \quad 1\ /(X \quad 1$. By making the substitution $Y \quad X \quad 1$ and using Eisenstein's criterion for the prime 5, we see that $(X^5 \quad 1\ /(X \quad 1$ is irreducible over $\mathbb{Q}$. This shows that $\mathbb{Q}\,\omega : \mathbb{Q} \quad 4$ and we deduce that $G \quad 4$. Finally we can define $\theta \quad G$ by $\theta(\omega \quad \omega^3$, because ω^3 is also a primitive 5th root of 1, and since $\theta^2(\omega \quad \omega^9 \quad \omega$, we deduce that $\theta^2 \quad 1$. We conclude that G has an element of order 4 and hence G is cyclic of order 4.

Fall 1993 Algebra Prelim Solutions

1. It is clear that Re is a left R-submodule of R, so we need to prove it is projective. It will be sufficient to show that Re is a direct summand of a free R-module. Since $R(1-e$ is also a left R-submodule of R, the result will be proven if we can show that $R \quad Re \quad R(1-e$. If $re \quad R(1-e$, then $re \quad s(1-e$ for some $s \quad R$ and so $re \quad ree \quad s(1-e\ e \quad 0$. This shows that $Re \quad R(1-e \quad 0$. Finally if $r \quad R$, then $r \quad r(e \quad 1-e \quad re \quad r(1-e$, so $R \quad Re \quad R(1-e$.

2. (a) Since we are in characteristic zero, everything is separable so we may use the theorem of the primitive element. This tells us that there exists $\alpha \quad K$ such that $K \quad F(\alpha$. If p is the minimal polynomial of α over F, then $K \quad F\ X\ /(p$.

   (b) Since p is the minimal polynomial, it is monic and irreducible in $F\ X$. Also we are in characteristic zero, so p is separable. This means that when we write $p \quad p_1 \ldots p_n$ in $K\ X$ where the p_i are monic irreducible polynomials, the p_i are distinct. Now write $c \quad f\ X \quad (p$ where $f \quad K\ X$. Since $c^2 \quad 0$, we see that $f^2 \quad (p$. Thus $f^2 \quad p_1 \ldots p_n q$ for some $q \quad K\ X$. By uniqueness of factorization, we have p_i divides f for all i and we deduce that $f \quad (p$. Therefore $c \quad 0$ as required.

3. (a) Suppose the action of $\mathrm{M}_2(\mathbb{Q}$ has a finite orbit with at least two elements. Using the formula that the number of elements in an orbit is the index of the stablizer of any element in that orbit, we see that $\mathrm{M}_2(\mathbb{Q}$ has a nontrivial subgroup H of finite index. Then $q\mathrm{M}_2(\mathbb{Q} \quad H$ for some positive integer q. However if $\alpha \quad \mathrm{M}_2(\mathbb{Q}$, then $\alpha \quad q(\alpha/q$, which shows that $q\mathrm{M}_2(\mathbb{Q} \quad \mathrm{M}_2(\mathbb{Q}$. We conclude that $\mathrm{M}_2(\mathbb{Q} \quad H$ and the result follows.

   (b) To check that we have an action, we must show that $(gh \quad \lambda \quad g \quad (h \quad \lambda$ for all $g,h \quad \mathrm{GL}_2(\mathbb{Q}$. This is true because

$$(g \quad h \ (\lambda \qquad \det(gh\ \lambda/\ \det(gh \qquad \det(g\ \det(h\ \lambda/(\ \det(g \quad \det(h$$
$$\det(g\ (h \quad \lambda\ /\ \det(g \qquad g \quad (h \quad \lambda$$

   Finally we see that all orbits have the form λ, and so in particular there are finite orbits which are not singletons.

4. By Sylow's theorem a group of order 34 has a normal subgroup of order 17, hence G has a normal subgroup H of order 17. Again by Sylow's theorem, this subgroup is the unique subgroup of G which has order 17. Since we are in characteristic zero, everything is separable and so L is a Galois extension of L^G. Therefore there is a one-one correspondence between the subfields of L containing L^G and the subgroups of G. This correspondence has the property that if A is a subgroup of G, then the dimension of L over L^A is A. The result follows by setting $K \quad L^H$.

5. Suppose S is not a field. Then it has a nonzero prime ideal P. Note that S/P is an integral domain. Since $S\ X\ /P\ X \qquad (S/P \quad X$, we see that $S\ X\ /P\ X$ is an integral domain which is not a field. We deduce that $P\ X$ is a nonzero nonmaximal prime ideal of $S\ X$. But nonzero prime ideals in a PID are maximal and since we are given that $S\ X$ is a PID, we now have a contradiction and the result follows.

6. (a) First H has an identity, namely the zero homomorphism defined by $0(a) = 0$ for all $a \in A$. If $f, g \in H$, then

$$\begin{aligned}(f+g)(a+b) &= f(a+b)+g(a+b) = f(a)+f(b)+g(a)+g(b)\\ &= f(a)+g(a)+f(b)+g(b) = (f+g)(a)+(f+g)(b)\end{aligned}$$

which shows that $f+g$ is a homomorphism, and so $f+g \in H$. Also if $f, g, h \in H$, then

$$\begin{aligned}((f+g)+h)(a) &= (f+g)(a)+h(a) = f(a)+g(a)+h(a)\\ &= f(a)+(g+h)(a) = (f+(g+h))(a),\end{aligned}$$

so $(f+g)+h = f+(g+h)$ which establishes the associative law. Finally for $f \in H$, the inverse of f is $-f$, where $(-f)(a) = -f(a)$. Since $(-f)(a+b) = -f(a+b) = -f(a)-f(b) = (-f)(a)+(-f)(b)$, we see that $-f \in H$, and we have established that H is a group.

(b) We first show that H is torsion free. If $f \in H$ has order $n \geq 1$, then $f(a) \neq 0$ for some $a \in A$. But then $(nf)(a) = n(fa) \neq 0$, a contradiction. Therefore the subgroup generated by $f_1, \ldots, f_m$ is a finitely generated torsion free abelian group, so by the fundamental structure theorem for finitely generated abelian groups it is free.

7. (a) A 2 by 2 matrix with entries in $\mathbb{Z}/p\mathbb{Z}$ will be invertible if and only if its columns are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. So there are p^2-1 choices for the first column (we cannot choose $(0,0)$ for the first column) and p^2-p choices for the second column (we cannot choose the vector in the first column). It follows that $G = (p^2-1)(p^2-p)$.

(b) Note that H is a Sylow p-subgroup of G, so the number of conjugates of H is congruent to 1 modulo p. Therefore 1 is congruent to 8 modulo p, which can only happen if $p \geq 7$. In the case $p \geq 7$, we have by Sylow's theorem that the number of conjugates of H in G is congruent to 1 modulo 7, which is of course congruent to 8 modulo 7. Thus the answer is $p \geq 7$.

a UFD. We now establish that $\mathbb{Z}[X]$ is not a PID by showing that the ideal $(2, X)$ (the ideal generated by 2 and X) is not principal.

Suppose on the contrary that $(2, X) = (f)$ for some $f \in \mathbb{Z}[X]$. Then there exist $g, h \in \mathbb{Z}[X]$ such that $fg = 2$ and $fh = X$. The equation $fg = 2$ shows that f must have degree 0, in other words $f \in \mathbb{Z}$, and then $fh = X$ shows that $f = \pm 1$. Thus we must have $(2, X) = \mathbb{Z}[X]$. Now the general element of $(2, X)$ is $2a + Xb$ where $a, b \in \mathbb{Z}[X]$. The constant term of $2a$ must be divisible by 2, and the constant term of Xb must be zero, hence the constant term of $2a + Xb$ must be divisible by 2. In particular we cannot have $2a + Xb = 1$, so $1 \notin (2, X)$ and we have the required contradiction.

5. Let G denote the Galois group of $x^3 - 10$ over $\mathbb{Q}$. By Eisenstein's criterion for the prime 2 (or otherwise), we see that $x^3 - 10$ is irreducible over $\mathbb{Q}$, hence $G = S_3$ or A_3. Let $\omega = (-1 + i\sqrt{3})/2$, a primitive cube root of unity. Then the roots of $x^3 - 10$ are $\sqrt[3]{10}$, $\omega\sqrt[3]{10}$, and $\bar{\omega}\sqrt[3]{10}$ ($\bar{\omega} = (-1 - i\sqrt{3})/2$), hence $x^3 - 10$ has one real root and two complex roots, so complex conjugation is an element of G. Therefore G has an element of order 2, which rules out the possibility $G = A_3$. Therefore $G = S_3$.

   A splitting field of $x^3 - 10$ is $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{10})$. The normal subfields of the splitting field correspond to normal subgroups of G. The normal subfields corresponding to the subgroups 1 and G are $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{10})$ and $\mathbb{Q}$ respectively. G has exactly one other normal subgroup, namely A_3, so there is exactly one other normal subfield. Since subfields of degree two over $\mathbb{Q}$ are always normal, this other normal subfield must be $\mathbb{Q}(i\sqrt{3})$.

6. (1) How to prove this depends on how much field theory one is allowed to assume. Also the result is true without the hypothesis that f is separable. Here is one way to proceed. Suppose K_1, K_2 are fields, $\theta: K_1 \to K_2$ is an isomorphism, $g \in K_1[X]$ is an irreducible polynomial, α_1 is a root of g in a splitting field L_1 for g, and α_2 is a root of the irreducible polynomial θg in a splitting field L_2 for θg (recall if $g = a_0 + a_1X + \cdots + a_nX^n$ with $a_i \in K_1$, then $\theta g = \theta a_0 + \theta a_1 X + \cdots + \theta a_n X^n \in K_2[X]$). Then θ extends to an isomorphism $\phi: K_1(\alpha_1) \to K_2(\alpha_2)$ such that $\phi(\alpha_1) = \phi(\alpha_2)$. Using induction on the degree of g, we deduce that ϕ in turn extends to an isomorphism of L_1 onto L_2. This is what is required.

   (2) Note that $x^4 - 2$ is indeed irreducible over $\mathbb{Q}$, by Eisenstein's criterion for the prime 2. The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Consider the permutation of the roots $\sqrt[4]{2} \to \sqrt[4]{2}$, $-\sqrt[4]{2} \to i\sqrt[4]{2} \to -i\sqrt[4]{2} \to -\sqrt[4]{2}$. This cannot be induced by an element θ of the Galois group of $x^4 - 2$ over $\mathbb{Q}$, because if $\theta\sqrt[4]{2} = \sqrt[4]{2}$, then we must have $\theta(-\sqrt[4]{2}) = -\sqrt[4]{2}$.

7. Since $\mathrm{Hom}_A(M, k) = 0$, we must have $M = \mathfrak{M}M$. Then Nakayama's lemma yields the result.

Spring 1994 Algebra Prelim Solutions

1. Suppose G is a simple group with exactly three elements of order two. Consider the conjugation action of G on the three elements of order two: specifically if $g \in G$ and x is an element of order two, then we define $g \cdot x = gxg^{-1}$. This action yields a homomorphism $\theta: G \to S_3$. Suppose $\ker\theta = G$. Then $gxg^{-1} = x$ for all $g \in G$ and for all elements x of order two. Thus if x is an element of order two, we see that x is in the center of G and hence G is not simple.

   On the other hand if $\ker\theta \neq G$, then since G is simple we must have $\ker\theta = 1$ and it follows that G is isomorphic to a subgroup of S_3. The only subgroup of S_3 which has exactly three elements of order two is S_3 itself. But S_3 is not simple (because A_3 is a nontrivial normal subgroup), hence G is not simple and the result is proven.

2. Let F denote the free group on generators x, y, and define a homomorphism $f: F \to S_3$ by $f(x) = (123)$ and $f(y) = (12)$. Since $f(x^6) = (123)^6 = e$, $f(y^4) = (12)^4 = e$, and $f(yxy^{-1}) = (213) = x^{-1}$, we see that f induces a homomorphism from G to S_3. This homomorphism is onto because its image contains $f(x) = (123)$ and $f(y) = (12)$, and the elements (123), (12) generate G. Thus G has a homomorphic image isomorphic to S_3.

   We prove that G is not isomorphic to S_3 by showing it has an element whose order is a multiple of 4 or ∞, which will establish the result because the orders of elements in S_3 are 1,2 and 3. We shall use bars to denote the image of a number in $\mathbb{Z}/4\mathbb{Z}$. Thus $\bar{0}$ is the identity of $\mathbb{Z}/4\mathbb{Z}$ under the operation of addition. Define $h: F \to \mathbb{Z}/4\mathbb{Z}$ by $h(x) = \bar{0}$ and $h(y) = \bar{1}$. Since $h(x^6) = 6\,\bar{0} = \bar{0}$, $h(y^4) = 4\,\bar{0} = \bar{0}$, and

$$h(yxy^{-1}) = \bar{1}\;\bar{0}-\bar{1}\;\bar{0} = h(x^{-1}),$$

   we see that h induces a homomorphism from G to $\mathbb{Z}/4\mathbb{Z}$, which has $\bar{1}$ in its image. Since $\bar{1}$ has order 4, it follows that G has an element whose order is either a multiple of 4 or infinity. This completes the proof.

3. (i) Since R is not a field, we may choose $0 \neq s \in R$ such that s is not a unit, equivalently $sR \neq R$. Define $f: R \to R$ by $f(r) = sr$. Then f is an R-module homomorphism which is injective, because R is a PID and $s \neq 0$, and is not onto because s is not a unit. This proves that R is isomorphic to the proper submodule sR of R.

   (ii) Using the fundamental structure theorem for finitely generated modules over a PID, we may write M as a direct sum of cyclic R-modules. Since M is not a torsion module, at least one of these summands must be R; in other words we may write $M = R \oplus N$ for some R-submodule N of M. Then $M \cong sR \oplus N$ and since $sR \oplus N$ is a proper submodule of $R \oplus N$, we have proven that M is isomorphic to a proper submodule of itself.

4. (i) We will write mappings on the left. Let $\beta: B \to B \oplus C$, $\gamma: C \to B \oplus C$ denote the natural injections (so $\beta b = (b,0)$), and let $\pi: B \oplus C \to B$, $\psi: B \oplus C \to C$ denote the natural epimorphisms (so $\pi(b,c) = b$). Define

$$\theta: \mathrm{Hom}_R(A, B \oplus C) \to \mathrm{Hom}_R(A,B) \oplus \mathrm{Hom}_R(A,C)$$

   by $\theta(f) = (\pi f, \psi f)$, and

$$\phi: \mathrm{Hom}_R(A,B) \oplus \mathrm{Hom}_R(A,C) \to \mathrm{Hom}_R(A, B \oplus C)$$

by $\phi(f,g) = \beta f + \gamma g$. It is easily checked that θ and ϕ are R-module homomorphisms, so will suffice to prove that $\theta\phi$ and $\phi\theta$ are the identity maps. We have

$$\theta\phi(f,g) = \theta(\beta f + \gamma g) = (\pi(\beta f + \gamma g), \psi(\beta f + \gamma g)) = (f,g)$$

because $\pi\gamma$, $\psi\beta$ are the zero maps, and $\pi\beta$, $\psi\gamma$ are the identity maps. Therefore $\theta\phi$ is the identity map. Also

$$\phi\theta(h) = \phi(\pi h, \psi h) = \beta\pi h + \gamma\psi h = (\beta\pi + \gamma\psi)h = h$$

because $\beta\pi + \gamma\psi$ is the identity map. Thus $\phi\theta$ is the identity map and (i) is proven.

(ii) Write $\mathrm{Hom}_R(A, A) = X$. If $\mathrm{Hom}_R(A, A) = A \oplus \mathbb{Z}$, then by the first part we would have $X = X \oplus \mathbb{Z}$. Thus $X = 0$, and we see that $\mathbb{Z}$ is the direct sum of two nonzero groups. This is not possible and the result follows.

5. (i) Let I be an ideal of $S^{-1}R$. We need to prove that I is finitely generated. Let $J = \{r \in R : r/1 \in S^{-1}I\}$ (where we view $S^{-1}R$ as elements of the form r/s where $r \in R$ and $s \in S$). Then J is an ideal of R and since R is Noetherian, there exist elements $x_1, \ldots, x_n$ which generate J as an ideal, which means $J = x_1R + \cdots + x_nR$. We claim that I is generated by $\{x_1/1, \ldots, x_n/1\}$. Indeed if $r/s \in I$, then $r = r_1x_1 + \cdots + r_nx_n$ for some $r_i \in R$, and hence $r/s = r_1/sx_1 + \cdots + r_n/sx_n$. This proves (i).

(ii) Let S be the multiplicative subset $\{1, X, X^2, \ldots\}$. Then every element of S is invertible in $R[X, X^{-1}]$ and hence the identity map $R[X] \to R[X]$ extends to a homomorphism $S^{-1}R[X] \to R[X, X^{-1}]$. It is easily checked that this map is an isomorphism. Since $R[X]$ is Noetherian, it follows from (i) that $S^{-1}R[X]$ is Noetherian and hence $R[X, X^{-1}]$ is Noetherian as required.

6. (i) Set $Y = X - 1$. Then

$$\begin{aligned} X^4 + X^3 + X^2 + X + 1 &= (X^5 - 1)/(X - 1) = ((Y+1)^5 - 1)/Y \\ &= (Y^5 + 5Y^4 + 10Y^3 + 10Y^2 + 5Y)/Y \\ &= Y^4 + 5Y^3 + 10Y^2 + 10Y + 5. \end{aligned}$$

Applying Eisenstein's criterion for the prime 5, we see that $Y^4 + 5Y^3 + 10Y^2 + 10Y + 5$ is irreducible in $\mathbb{Q}[Y]$. Since $Y \to Y + 1$ induces an automorphism of $\mathbb{Q}[Y]$, we deduce that $X^4 + X^3 + X^2 + X + 1$ is irreducible.

(ii) Let $c(X)$ denote the characteristic polynomial of A, and let $m(X)$ denote the minimum polynomial of A. Since $A^5 = I$, we see that $m(X)$ divides $X^5 - 1$, and since 1 is not an eigenvalue of A, we see that $X - 1$ does not divide $m(X)$. Therefore $m(X)$ divides $X^4 + X^3 + X^2 + X + 1$ and using (i), we deduce that the only irreducible factor of $m(X)$ is $X^4 + X^3 + X^2 + X + 1$. It follows that the only irreducible factor of $c(X)$ is $X^4 + X^3 + X^2 + X + 1$, which shows that the degree of $c(X)$ is a multiple of 4. This completes the proof, because n is the degree of $c(X)$.

Fall 1994 Algebra Prelim Solutions

1. (i) By definition $\mathfrak{C}(x) = \{gxg^{-1} \mid g \in G\}$. Since $x \in H \lhd G$, we see that $gxg^{-1} \in H$ for all $g \in G$ and we deduce that $\mathfrak{C}(x) \subseteq H$. Let $C_G(x)$ denote the centralizer of x in G. Then $|\mathfrak{C}(x)| = |G : C_G(x)|$. This last quantity is a power of p and it cannot be 1 because x is not in the center of G. We deduce that $|\mathfrak{C}(x)|$ is a nontrivial power of p and (i) follows.

   (ii) It follows from (i) that $H - Z$ is a union of conjugacy classes of the form $\mathfrak{C}(x)$ where $x \in H - Z$. Since different conjugacy classes intersect trivially, we see from (i) that p divides $|H - Z|$. Also $|H|$ divides $|G|$ and so $|H|$ is a nontrivial power of p. We deduce that p divides $|Z| - |H|$ and (ii) is proven.

   (iii) Let H be the centralizer of A in G. Then H is a normal subgroup of G containing A and it will be sufficient to show that $H = A$. Let X/A be the center of G/A and suppose $H \neq A$. Then we see from (ii) that $|X/A| - |H/A| \neq 1$ because $H/A \lhd G/A$, and we deduce that there is a nontrivial cyclic subgroup Y/A contained in $X/A - H/A$. Since $Y/A \leqslant X/A$ we see that $Y/A \lhd G$ and we deduce that $Y \lhd G$. Also A is contained in the center of Y and Y/A is cyclic, hence Y is abelian. This contradicts the fact that A is a maximal normal abelian subgroup of G and the result follows

2. (i) The number of Sylow 5-subgroups of G divides 36 and is congruent to 1 modulo 5, which means that this number must be 1,6 or 36. It cannot be 1, for then G would have a normal Sylow 5-subgroup, which contradicts the fact that G is simple. Nor can G have 6 Sylow 5-subgroups, for then G would be isomorphic to a subgroup of A_6 because G is simple. This would mean that A_6 has a subgroup of index 2, and since subgroups of index 2 are always normal, this would contradict the fact that A_6 is simple. We conclude that G has 36 Sylow 5-subgroups.

   (ii) Let N be the normalizer of a Sylow 3-subgroup. Then the number of Sylow 3-subgroups is $|G : N|$. Also the number of Sylow 3-subgroups divides 20 and is congruent to 1 modulo 3, so this number is 1,4 or 10. It cannot be 1 because that would mean G has a normal Sylow 3-subgroup, which would contradict the fact that G is simple. Nor can it be 4, for then G would be isomorphic to a subgroup of A_4 because G is simple, which is clearly impossible. Therefore the number of Sylow 3-subgroups is 10. We deduce that $|G : N| = 10$ and hence N has order 18.

   (iii) A Sylow 3-subgroup of a group of order 18 has order 9. This means the subgroup has index 2, hence the subgroup is normal because in any group, a subgroup of index 2 is normal.

   (iv) Let C be the centralizer in G of $A \cap B$ and suppose $A \cap B$ is not 1. Then C contains A, B and $A \cap B$ is a normal subgroup in C, so C cannot be the whole of G. Therefore the order of C is a multiple of 9 and divides 180, and is neither 9 nor 180. Let d be the index of C in G, so $|C| = |G|/d$. Then G is isomorphic to a subgroup of A_d because G is simple. Since the order of A_d is less than 180 if $d < 5$, we see that $d = 6$ and consequently C has order 18. From part (iii), the Sylow 3-subgroup of C is normal in C and therefore C has exactly one subgroup of order 9. We now have a contradiction because C has two subgroups of order 9, namely A and B. We conclude that $A \cap B = 1$.

   (v) We count the elements in G. Since two Sylow 5-subgroups intersect in 1 and there are 36 Sylow 5-subgroups by (i), we see that G has $36 \cdot 4 = 144$ elements of order 5. Also

two Sylow 3-subgroups intersect in 1 by (iv) and G has 10 Sylow 3-subgroups by (ii). Therefore G has 8 10 80 elements of order 3 or 9. We conclude that G has at least 144 80 224 elements, which contradicts the fact that G has only 180 elements. It follows that no such G can exist and thus there is no simple group of order 180.

3. Since M is a cyclic R-module, we know that $M \cong R/Rs$ for some $s \in R$. By the uniqueness part of the fundamental structure theorem for finitely generated modules over a PID, we cannot write $R \cong A \oplus B$ where A, B are nonzero R-modules. Therefore $s \neq 0$. Since $sM = 0$, we may take $r = s$.

   Since $rM = 0$, we see that $rR \subseteq sR$ and hence s divides r. Suppose there do not exist distinct primes p, q dividing r. Then the same is true for s because s divides r, and we deduce that s is a prime power, say p^e for some prime p. From the uniqueness statement in the fundamental structure theorem for finitely generated modules over a PID, we cannot write $R/Rp^e \cong A \oplus B$ where A, B are nonzero R-modules and we have a contradiction. This finishes the proof.

4. (i) Choose integers r, s such that $qr \equiv 2s \equiv 1$. Then in $\mathbb{Z}[X]/(X-2)$ we have $qr \equiv 1 - sX \bmod (X-2)$. Since $1 - sX$ is invertible in $\mathbb{Z}[X]$ (with inverse $1 + sX + s^2X^2 + \cdots$), it follows that q is invertible in $\mathbb{Z}[X]/(X-2)$.

   (ii) The general element of R is $\sum a_i X^i \bmod (X-2)$, where $a_i \in \mathbb{Z}_{(2)}$ for all i. Now each a_i is of the form p/q where $p, q \in \mathbb{Z}$ and q is odd. Using (i), we may now write $a_i \equiv b_i \bmod (X-2)$ where $b_i \in \mathbb{Z}$, and then we may write the general element of R in the form $\sum b_i X^i \bmod (X-2)$. This proves that $\pi\theta$ is surjective. We now determine the kernel of $\pi\theta$. Obviously $(X-2) \subseteq \ker \pi\theta$. Conversely suppose $f \in \ker \pi\theta$. Then we may write $f = (X-2)g$ where $g \in \mathbb{Z}_{(2)}[X]$. We want to show that $g \in \mathbb{Z}[X]$. Write $g = \sum g_i X^i$ where $g_i \in \mathbb{Z}_{(2)}$. Then the coefficient of X^n in $g(X-2)$ is $g_{n-1} - 2g_n$ for $n \geq 0$, and the constant coefficient is $-2g_0$. By induction on n we see that $2g_n \in \mathbb{Z}$ and since $g_n \in \mathbb{Z}_{(2)}$, we conclude that $g_n \in \mathbb{Z}$ for all n. This proves that $\ker \pi\theta = (X-2)$ and it now follows from the fundamental isomorphism theorem that $R \cong \mathbb{Z}[X]/(X-2)$.

   (iii) By considering the homomorphism $\mathbb{Z}[X] \to \mathbb{Z}$ determined by sending X to 2, we see that $\mathbb{Z}[X]/(X-2) \cong \mathbb{Z}$. Since 3 is not invertible in $\mathbb{Z}$, we see that 3 is not invertible in $\mathbb{Z}[X]/(X-2)$. But 3 is invertible in R and the result follows.

5. (i) Obviously $K(\alpha^p) \subseteq K(\alpha)$. Also α is separable over $K(\alpha^p)$ and satisfies the polynomial $X^p - \alpha^p$. Since α is the only root of $X^p - \alpha^p$, it follows that $\alpha \in K(\alpha^p)$ and hence $K(\alpha) = K(\alpha^p)$.

   Now we consider the minimum polynomial of β over K. This has degree p because $[K(\beta) : K] = p$, and must be a polynomial in X^p because β is not separable over K. Thus the minimum polynomial must be of the form $X^p - b$ for some $b \in K$ and it follows that $\beta^p = b \in K$.

   (ii) Since we are in characteristic p, we have $(\alpha + \beta)^p = \alpha^p + \beta^p$. But $\beta^p \in K$ by (i), hence $\alpha^p \in K(\alpha + \beta)$. Therefore $K(\alpha^p) \subseteq K(\alpha + \beta)$ and it now follows from (i) that $K(\alpha) \subseteq K(\alpha + \beta)$ as required.

   (iii) Since $K(\alpha + \beta) \subseteq K(\alpha)$ by (ii), we have $[K(\alpha + \beta) : K] \leq [K(\alpha + \beta) : K(\alpha)][K(\alpha) : K]$ and since $[K(\alpha) : K] = d$, it remains to prove that $[K(\alpha + \beta) : K(\alpha)] \leq p$. Now $(\alpha + \beta)^p = \alpha^p + \beta^p \in K(\alpha)$ which shows that $[K(\alpha + \beta) : K(\alpha)] = p$ or 1, because we

are in characteristic p. It remains to prove that $K(\alpha \quad \beta : K(\alpha \quad 1$, or equivalently that $\beta / K(\alpha$. But α is separable over K, hence every element of $K(\alpha$ is separable over K which shows that $\beta / K(\alpha$ because β is not separable over K. This completes the proof.

6. (i) It will be sufficient to prove that $X^p - t$ is irreducible in t, X , or equivalently that $t - X^p$ is irreducible in X, t . Let $R \quad X$ and let $F \quad (X$, the field of fractions of R. Then $t - X^p$ is a monic polynomial in $R\,t$ and is irreducible in $F\ t$, hence it is irreducible in $R\,t \quad X, t$ and the result follows.

   (ii) Let y be one of the roots of $X^p - t$ in L. Since $X^p - t$ is irreducible in $K\ X$, we see that $K(y \ : K \quad p$. Also the roots of $X^p - t$ are $e^{2n\pi i/p} y$ where $n \quad 0, \ldots, p-1$, and since $e^{2n\pi i/p}$ for all n, we deduce that all the roots of $X^p - t$ are in $K(y$. It follows that $K(y \quad L$ and we conclude that $L : K \quad p$. Therefore the Galois group of L over K has order p (note that L/K is a separable extension because we are in characteristic zero). Since groups of order p are cyclic, we conclude that the Galois group of L over K is cyclic of order p and hence isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Spring 1995 Algebra Prelim Solutions

1. Let G be a group of order $1127 = 7^2 \cdot 23$. The number of Sylow 23-subgroups divides 49 and is congruent to 1 modulo 23. This means that G has exactly one Sylow 23-subgroup and therefore G has a normal Sylow 23-subgroup A. Also the number of Sylow 7-subgroups divides 23 and is congruent to 1 modulo 23. Therefore the number of Sylow 7-subgroups is 1 and we deduce that G has a normal Sylow 7-subgroup B.

   Since G has normal subgroups A, B such that $A \cap B = 1$ and $G = AB$, we see that $G \cong A \times B$. Now groups of prime order p are isomorphic the cyclic group $\mathbb{Z}/p\mathbb{Z}$, while groups of order p^2 are either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Therefore G is isomorphic to either $\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$. In particular G is abelian and by the fundamental structure theorem for finitely generated abelian groups, these last two groups are not isomorphic. Therefore up to isomorphism there are two groups of order 1127, namely $\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$.

2. We shall prove the result by induction on $|G|$, the result being obviously true if $|G| = 1$. Also if G is abelian, then there is nothing to prove, so we may assume that G is not abelian. Since G is nilpotent and not 1, its center Z is not 1. By induction the result is true for G/Z. Note that if G/Z is cyclic, then G is abelian which is not the case. Therefore G/Z is noncyclic. By induction, G/Z has a normal subgroup H/Z such that $(G/Z)/(H/Z)$ is a noncyclic abelian group. But $(G/Z)/(H/Z) \cong G/H$ and the result follows.

3. Let G be a finitely generated abelian group with the given property. Then by the structure theorem, G is isomorphic to a direct product of nontrivial groups $A_1, A_2, \ldots, A_n$ of prime power order. If $n > 1$, then $A_1 \subset A_2$ and $A_2 \subset A_1$. Therefore $n = 1$. This means that G is cyclic of prime power order. Conversely if G is cyclic of prime power order, it has the given property, because then G has exactly one subgroup of each order dividing $|G|$ and it follows that G has the property as stated in the problem. We conclude that the finitely generated abelian groups with the property that for all subgroups A, B, either $A \subset B$ or $B \subset A$ are the cyclic groups of prime power order.

4. (a) Let $x \in R/\operatorname{rad} I$ and suppose $x^n = 0$ where $n > 0$. Then we may write $x = y + \operatorname{rad} I$ where $y \in R$. Since $x^n = 0$, we see that $y^n \in \operatorname{rad} I$, which means that $y^n \in \operatorname{rad} I$. By definition of $\operatorname{rad} I$ we see that $(y^n)^m = 0$. Therefore $y^{mn} = 0$, hence $y \in \operatorname{rad} I$ and we deduce that $x = 0$. This establishes that $R/\operatorname{rad} I$ has no nonzero nilpotent elements.

   (b) If $x \in P_1 \cap P_2 \cap \cdots \cap P_n$, then $x \in P_i$ for all i and hence $x^n \in P_1 P_2 \cdots P_n$. It follows that $x \in \operatorname{rad}(P_1 P_2 \cdots P_n)$. Conversely suppose $x \in \operatorname{rad}(P_1 P_2 \cdots P_n)$. Then $x \in \operatorname{rad} P_i$ for all i. This means that $x^m \in P_i$ for some $m > 0$ and since P_i is prime, we deduce that $x \in P_i$ for all i as required.

   (c) If P_i is contained in every P_j, then $P_1 \cap \cdots \cap P_n \subset P_i$ and hence $R/\operatorname{rad}(P_1 \cdots P_n) \subset R/P_i$ by (b). We deduce that $R/\operatorname{rad}(P_1 \cdots P_n)$ is an integral domain.

   Conversely suppose $R/\operatorname{rad}(P_1 \cdots P_n)$ is an integral domain. Then by (b) we see that $R/(P_1 \cap \cdots \cap P_n)$ is also an integral domain. Suppose there does not exist an i such that P_i is contained in P_j for all j. Then for each i, we can choose $x_i \in P_i$ such that $x_i \notin P_j$ for some j (where j depends on i). Now set $y_i = x_i + P_1 \cap \cdots \cap P_n$ for $i = 1, \ldots, n$. Then y_i is

a nonzero element of $R/(P_1 \cdots P_n$ for all i, yet

$$y_1 \cdots y_n \quad x_1 \cdots x_n \quad P_1 \quad \cdots \quad P_n \quad 0$$

This shows that $R/(P_1 \cdots P_n$ is not an integral domain and we have a contradiction. This completes the proof.

5. Obviously $K(\alpha^3 \quad K(\alpha$. Now

$$8 \quad K(\alpha : K \quad K(\alpha : K(\alpha^3 \quad K(\alpha^3 : K$$

which shows that $K(\alpha : K(\alpha^3$ divides 8. Also α satisfies the polynomial $X^3 - \alpha^3$ which shows that $K(\alpha : K(\alpha^3 \quad 3$. Therefore $K(\alpha : K(\alpha^3 \quad 1$ or 2. We need to eliminate the possibility that $K(\alpha : K(\alpha^3 \quad 2$. If $K(\alpha : K(\alpha^3 \quad 2$, then the polynomial $X^3 - \alpha^3$ could not be irreducible over $K(\alpha^3$, and it would follow that $X^3 - \alpha^3$ has a root in $K(\alpha^3$. But the roots of $X^3 - \alpha^3$ are $\alpha, \omega\alpha$ and $\omega^2\alpha$ and since $\omega \quad K$, it would follow that all the roots of $X^3 - \alpha^3$ are in K. In particular $\alpha \quad K(\alpha^3$. This establishes the result.

6. (a) Let T denote the ideals of R which have trivial intersection with S. Since a is not nilpotent, we see that $0 \notin S$ and hence $0 \quad T$. Therefore T is nonempty. Moreover T is ordered by inclusion, and the union of a chain in T is still in T. It now follows from Zorn's lemma that T has maximal elements; let P be one of these maximal elements. Then $P \quad S \quad \emptyset$. We claim that P is prime. If P is not a prime ideal, then there exist ideals A, B strictly containing P such that $AB \quad P$. By maximality of P we have $a^i \quad A$ and $a^j \quad B$ for some i, j and hence $a^{i \quad j} \quad P$. This contradicts the fact that $P \quad T$, and it follows that P is a prime ideal not containing a.

   (b) Let $\theta\colon R \quad K$ denote the composition of the natural epimorphism $R \quad R/P$ followed by the natural monomorphism $R/P \quad K$. If $b \quad S$, then $b \notin P$, hence the image of b in R/P is nonzero and we deduce that θb is invertible in K. It follows that θ extends to a ring homomorphism $\phi\colon S^{-1}R \quad K$.

7. (a) The proper subfields of F containing K are in a one-one correspondence with the proper subgroups of $\mathrm{Gal}(F/K$. Therefore we need to show that S_4 has at least 9 proper subgroups. There are 6 elements of order 2 and 8 elements of order 3 in S_4. Since any two subgroups of order 2 or 3 intersect in the identity, we see that there are 6 subgroups of order 2 and 4 subgroups of order 3, and we have shown that $\mathrm{Gal}(F/K$ has at least 10 proper subgroups. This finishes part (a).

   (b) The Galois extensions E of K in F correspond to the normal subgroups of $\mathrm{Gal}(F/K$, so we need a nontrivial normal subgroup of $\mathrm{Gal}(F/K$. The simplest one is the alternating subgroup A_4 of S_4. The corresponding subfield E of K is the elements of F fixed by A_4. Also $\mathrm{Gal}(E/K \quad S_4/A_4 \quad \mathbb{Z}/2\mathbb{Z}$.

8. First we find the Jordan canonical form of the matrix $\begin{matrix} 0 & -2 \\ 1 & 3 \end{matrix}$ The characteristic equation of this matrix is $-x(3-x \quad 2 \quad 0$, which has roots 1 and 2. Therefore the Jordan canonical

form of this matrix is $\begin{matrix} 1 & 0 \\ 0 & 2 \end{matrix}$ and we deduce that the Jordan canonical form of A is

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

The matrices which commute with this canonical form are the matrices of the form

$$\begin{matrix} p & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{matrix}$$

where p, a, b, c, d are arbitrary complex numbers.

Fall 1995 Algebra Prelim Solutions

1. The order of G is $5^3 \cdot 7^3$. The number of Sylow 5-subgroups of G divides 7^3 and is congruent to 1 modulo 5; the only possibility is 1. Therefore G has a normal Sylow 5-subgroup A. The number of Sylow 7-subgroups of G divides 5^3 and is congruent to 1 modulo 7; the only possibility is 1. Therefore G has a normal Sylow 7-subgroup B.

   Since (A , B 1, we see that A B 1. We next show that every element of A commutes with every element of B. Suppose a A and b B. Then $aba^{-1}b^{-1}$ $a(ba^{-1}b^{-1}$ and since $A \lhd G$, we see that $ba^{-1}b^{-1}$ A and consequently $aba^{-1}b^{-1}$ A. Similarly $aba^{-1}b^{-1}$ B and we deduce that $aba^{-1}b^{-1}$ A B 1. Therefore $aba^{-1}b^{-1}$ 1 and we conclude that ab ba, in other words every element of A commutes with every element of B.

   Since a group of prime power order has normal subgroups of order m for all m dividing the order of the group, we see that A has a normal subgroup H of order 25. From the previous paragraph, B centralizes H and so certainly normalizes H. Thus A and B normalize H, hence A and B divide the order of the normalizer of H in G and we conclude that $H \lhd G$. This completes the solution.

2. First we write G as a direct product of cyclic groups of prime power order: G $\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/9\mathbb{Z}$ $\mathbb{Z}/9\mathbb{Z}$ $\mathbb{Z}/5\mathbb{Z}$. Any subgroup of G is isomorphic to a product of subgroups, where one subgroup is taken from each factor. Thus H $\mathbb{Z}/9\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$ $\mathbb{Z}/9\mathbb{Z}$. These last two groups are isomorphic, so we conclude that H $\mathbb{Z}/3\mathbb{Z}$ $\mathbb{Z}/9\mathbb{Z}$.

3. (a) Since D is a conjugacy class in $f^{-1}(C$, we may write D bdb^{-1} b $f^{-1}(C$ for some fixed d D. Then

   $$f(D \quad f(bdb^{-1} \quad f(b\ f(d\ f(b^{-1}\ b \quad f^{-1}(C \quad .$$

   Therefore $f(D$ $cf(d\ c^{-1}\ c$ C , and (a) follows.

   (b) Let $D(g$ denote the conjugacy class of g in $f^{-1}(C$. Since $f(g$ is centralized by C, the conjugacy class containing $f(g$ is precisely $f(g$. Since $f(D(g$ is by (a) the conjugacy class containing $f(g$, we see that $f(D(g$ 1. Therefore all elements of $D(g$ are in the same coset of $\ker f$ and we conclude that $D(g$ $\ker f$ as required.

   (c) Let K denote the centralizer of g in $f^{-1}(C$. Then the order of the centralizer of g in G is at least K . Now the order of the conjugacy class of g in $f^{-1}(C$ is $f^{-1}(C$ $:K$, and by (b) this order is at most $\ker f$. Therefore $f^{-1}(C$ $:K$ $\ker f$, consequently

   $$K \quad f^{-1}(C\ /\ker f \quad C$$

   because $f^{-1}(C\ /\ker f$ C. The result follows.

4. (a) If R has no prime elements, then R is a field and so certainly a PID. Therefore we may suppose that R has exactly one prime p (up to a multiple of a unit), and we need to prove that R is a PID. Let I be a nonzero ideal of R. Then each nonzero element of I can be written in the form up^n for some nonnegative integer n and some unit u, because p is the only prime (up to a multiple of a unit) of R. Let N be the smallest nonnegative integer such that up^N I for some unit u. We now show that I $p^N R$; clearly $p^N R$ I. If x I 0, then we may write x vp^n for some unit v and some integer n N. Thus x $p^N vp^{n-N}$ which shows that x $p^N R$, and the result follows.

(b) Suppose every maximal ideal of R is principal. Then each maximal ideal of R is of the form pR where p is a prime of R. Suppose by way of contradiction that I is a nonprincipal ideal of R. Clearly $0 \quad I \quad R$. Choose a nonzero element $x \quad I$, and write $x \quad p_1^{d_1} \dots p_n^{d_n}$, where the p_i are nonassociate primes and the d_i are positive integers.

For each prime p, let $e(p$ denote the largest integer such that $p^{e(p} \; R \quad I$. If p is not an associate of one of the p_i, then $e(p \quad 0$. Set $y \quad p_1^{e_1} \dots p_n^{e_n}$. We claim that $I \quad yR$.

First we show that $I \quad yR$. If $z \quad I$, then by unique factorization we may write $z \quad qp_1^{f_1} \dots p_n^{f_n}$, where the f_i are nonnegative integers and q is a product of primes which are not associate to any of the p_i. Again using unique factorization, we must have $f_i \quad e_i$ for all i and we deduce that $z \quad yR$.

Finally we show that $yR \quad I$. Set $J \quad r \quad R \;\; yr \quad I$ (so $J \quad y^{-1}I$). Clearly J is an ideal of R and $yJ \quad I$. If $J \quad R$, then by Zorn's lemma J is contained in a maximal ideal of R, which we may assume is of the form pR where p is a prime of R. It would follow that $ypR \quad I$, which contradicts the maximality of the $e(p$. Therefore $J \quad R$ and we deduce that $yR \quad I$. Thus $I \quad yR$ and the proof is complete.

5. Let $\pi\colon N \quad X \quad N$ denote the projection onto N, so $\pi(n,x \quad n$ for all $n \quad N$ and $x \quad X$, and let ι denote the identity map on N. Then $(\pi f \; i \quad \pi\sigma \quad \iota$. This shows that i has a left inverse, consequently the sequence

$$0 - \quad N \; -^{i} \quad M - \quad M/N - \quad 0$$

splits (the map $M \quad M/N$ above is of course the natural epimorphism). This shows that $M \quad N \quad M/N$ as required.

6. Let G denote the Galois group of E over F. Since E is a Galois extension of F with $E : F \quad p^n$, we see that $G \quad p^n$. Since G is a p-group, it has a series $G \quad G_0 \quad G_1 \quad \cdots \quad G_{n-1} \quad G_n \quad 1$, with $G_i \lhd G$ and $G_i/G_{i-1} \quad p$ for all i. Set $K_i \quad e \quad E \;\; ge \quad e$ for all $g \quad G_i$. Then by the Galois correspondence, K_i is normal over F and $K_i : K_{i-1} \quad G_i : G_{i-1} \quad p$ for all i, as required.

7. Suppose K is a finite field which is algebraically closed. Let n be a positive integer which is prime to the characteristic of K, and consider the polynomial $X^n - 1$. The derivative of $X^n - 1$ is nX^{n-1} which is prime to $X^n - 1$ in $K \; X$, because n is prime to the characteristic of K. This tells us that the roots of $X^n - 1$ in a splitting field for K are distinct. If K is algebraically closed, then all these roots would be in K, and we would deduce that $K \quad n$. Since n can be arbitrarily large, this would contradict the assumption that K is finite, and the result is proven.

January 1996 Algebra Prelim Solutions

1. Since f is an epimorphism from G to H, the fundamental isomorphism theorem tells us that $G/\ker f \cong H$, so in particular $|G/\ker f| = |H|$. Therefore $|G| / |\ker f| = |H|$, hence $|\ker f| = |G| / |H|$ and we deduce that $|\ker f| = 3^3 \cdot 11^2$. Using the fundamental theorem for finitely generated abelian groups, we see that there are up to isomorphism six abelian groups of order $|\ker f| = 3^3 \cdot 11^2$, namely

$\mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/121\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/121\mathbb{Z}$	$(\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/121\mathbb{Z}$
$\mathbb{Z}/27\mathbb{Z} \times (\mathbb{Z}/11\mathbb{Z})^2$	$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/11\mathbb{Z})^2$	$(\mathbb{Z}/3\mathbb{Z})^3 \times (\mathbb{Z}/11\mathbb{Z})^2$

2. (i) Since $A \cap B$ is a subgroup of G whose order divides $|A| = p^4$ and $|B| = q^5$, we see that $|A \cap B| = 1$ and hence $A \cap B = 1$. Next if $a \in A$ and $b \in B$, then $a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)\, b \in B$, because $B \lhd G$. Similarly $a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in A$ and we deduce that $a^{-1}b^{-1}ab \in A \cap B = 1$. Therefore $a^{-1}b^{-1}ab = 1$, consequently $ab = ba$ for all $a \in A$ and $b \in B$. We can now define a map $\theta: A \times B \to G$ by $\theta(a,b) = ab$. Then

$$\theta\big((a_1,b_1)(a_2,b_2)\big) = \theta(a_1a_2,b_1b_2) = a_1a_2b_1b_2 = (a_1b_1)(a_2b_2)$$

(because a_2 commutes with b_1), hence $\theta\big((a_1,b_1)(a_2,b_2)\big) = \theta(a_1,b_1)\,\theta(a_2,b_2)$ and we deduce that θ is a homomorphism. If $(a,b) \in \ker\theta$, then $ab = 1$ and so $a = b^{-1}$. Thus $a = b^{-1} \in A \cap B = 1$ and we deduce that $a = b = 1$. Therefore $\ker\theta = 1$ and so θ is a monomorphism. Since $|G| = |A \times B|$ we conclude that θ is also onto, consequently θ is an isomorphism and the result follows.

(ii) Since A is a p-group, it has a normal subgroup P of order p. Similarly B has a normal subgroup Q of order q. Since $P \times Q$ is a normal subgroup of $A \times B$ of order pq, we see that $\theta(P \times Q)$ is a normal subgroup of G of order pq, and so we may set $N = P \times Q$ to satisfy the requirements of the problem.

3. Let G be a simple group of order $2^2 \cdot 3 \cdot 11^2$. The number of Sylow 11-subgroups is congruent to 1 modulo 11 and divides 12, so the possibilities are 1 and 12. If there is 1 Sylow 11-subgroup, then it would have to be normal, which is not possible because G is simple. Therefore there are 12 Sylow 11-subgroups. If N is the normalizer of a Sylow 11-subgroup, then $|G:N|$ is the number of Sylow 11-subgroups, so $|G:N| = 12$. By considering the permutation representation of G on the left cosets of N in G and using the fact that G is simple, we see that there is a monomorphism of G into A_{12}, the alternating group of degree 12. This means that G is isomorphic to a subgroup of A_{12}. This is not possible because 121 divides $|G|$, but 121 does not divide $|A_{12}|$. We now have a contradiction and we deduce that no such G exists, as required.

4. Since $(\sqrt{2}\sqrt{3})^3 - 9(\sqrt{2}\sqrt{3}) = 2\sqrt{2}$, we see that $\sqrt{2} \in \mathbb{Q}(\sqrt{2}\sqrt{3})$ and we deduce that $\mathbb{Q}(\sqrt{2}\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Now $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, and $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 1$ or 2, because $\sqrt{3}$ satisfies $x^2 - 3$, a degree 2 polynomial over $\mathbb{Q}(\sqrt{2})$. Therefore $[\mathbb{Q}(\sqrt{2}\sqrt{3}):\mathbb{Q}] = 4$ or 2, depending on whether or not $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then we may write $\sqrt{3} = a + b\sqrt{2}$ where $a,b \in \mathbb{Q}$. Clearly $a,b \neq 0$. Squaring we obtain $3 = a^2 + 2ab\sqrt{2} + 2b^2$ and we deduce that $\sqrt{2}$ is rational, which is not so.

Therefore $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and consequently $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq 4$. Note we also have that $1, \sqrt{2}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2})$, and $1, \sqrt{3}$ is a $\mathbb{Q}(\sqrt{2})$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall that if e_i is an F-basis for E over F and f_j is an E-basis for K, then $e_i f_j$ is an F-basis for K. It follows that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

5. Let P be a prime ideal of D and suppose P was not maximal. Then there would exist $M \lhd D$ such that $M \neq D$ and M properly containing P. Since D is a PID, we may write $P = pD$ and $M = mD$ for some $m, p \in D$ with $p \neq 0$. Then $p = mx$ for some $x \in D$ because M contains P. Since P is a prime ideal, we must have m or $x \in P$. We cannot have $m \in P$ because M properly contains P. Therefore we must have $x \in P$ and then we may write $x = py$ for some $y \in D$. This yields $p = mpy$ and since D is a domain, we see that $1 = my$. This shows that $mD = D$, which contradicts the fact that M is a proper ideal of D and the first part of the problem is proven.

   Suppose now that $f : D \to K$ is a ring epimorphism onto the integral domain K with $\ker f \neq 0$. Then $D/\ker f \cong K$, so $\ker f$ is a prime ideal because $D/\ker f$ is an integral domain. Using the first part of the problem, we see that $\ker f$ is a maximal ideal of D. Therefore $D/\ker f$ is a field and it follows that K is a field as required.

   For the last part a counterexample is $R = \mathbb{Z}/6\mathbb{Z}$. Let P be the prime ideal $2\mathbb{Z}/6\mathbb{Z}$, Q the prime ideal $3\mathbb{Z}/6\mathbb{Z}$, and $S = R \setminus P$. Note that the ideals of R are precisely 0, R, P and Q, and the prime ideals of R are precisely P and Q. Then $S^{-1}P = 0$ because $s + 6\mathbb{Z} \neq 3 + 6\mathbb{Z}$ S and $sp = 0$ for all $p \in P$, and $S^{-1}Q = R_P$ because $Q \cap S = \emptyset$. Since all ideals of R_P are of the form $S^{-1}I$ for some $I \lhd R$, we see that 0 and R_P are the only ideals of R_P and it follows that R_P is a field. Similarly R_Q is a field. Since R is not an integral domain, we have now established that R is a counterexample.

6. Suppose P is a prime ideal of R and R_P has a nonzero nilpotent element. Then we may assume that R_P has a nonzero element α such that $\alpha^2 = 0$. If $S = R \setminus P$, then we may write the nilpotent element as r/s where $r \in R$ and $s \in S$. Since $(r/s)^2 = 0$, we see that $r^2 t = 0$ for some $t \in S$, and $rt \neq 0$ because $r/s \neq 0$. Also $(rt)^2 = r^2 t^2 = 0$, so rt is a nonzero nilpotent element of R.

   Suppose r is a nonzero nilpotent element of R. It remains to prove that R_P has a nonzero nilpotent element for some prime ideal P of R. We may assume that $r^2 = 0$. Let $I = \{s \in R : rs = 0\}$, an ideal of R which does not contain 1. By Zorn's lemma, there is a maximal ideal P of R containing I; of course P will also be a prime ideal. Then the image $r/1$ in R_P is nonzero because $rt \neq 0$ for all $t \in R \setminus P$. Since $(r/1)^2 = r^2/1^2 = 0/1^2 = 0$, we see that $r/1$ is a nonzero nilpotent element of R_P. This completes the proof.

7. The submodule of M generated by A and B is $A + B$; this is the set $\{a + b : a \in A \text{ and } b \in B\}$. Thus we need to prove that $A + B \cong A \oplus B$. We define a map $\theta : A \oplus B \to M$ by $\theta(a, b) = a + b$. Clearly this is an R-module homomorphism of $A \oplus B$ onto $A + B$. If $(a, b) \in \ker\theta$, then $a + b = 0$, consequently $a = -b$. This shows that a and $-b$ are both in $A \cap B = 0$. Therefore $a = b = 0$ and hence $\ker\theta = 0$. It follows that θ is an isomorphism and so $A + B \cong A \oplus B$ as required.

8. (i) Since there is a one-one correspondence between the subgroups of $\mathrm{Gal}(E/F)$ (the Galois group of E over F) and the proper subfields of E containing F, we need to show that S_6 has at

least 35 proper subgroups. One way to do this is to note that S_6 has 144 5-cycles which gives 36 subgroups of order 5.

(ii) The subfield L required is Fix$(A_6$, the subset of E which is fixed pointwise by all elements of the alternating subgroup A_6 of S_6. Since A_6 is a normal subgroup of S_6, we see that L is a Galois extension of F, and that Gal$(E/L$ A_6. Since A_6 is a simple group, there is no subfield between E and L which is Galois over L.

(iii) The dimension of L over F is S_6/A_6 2.

August 1997 Algebra Prelim Solutions

1. (a) Obviously $0 \in IJ$. Now suppose $x, y \in IJ$ and $r \in R$. We want to prove that $x - y, rx \in IJ$. Write $x = \sum_{i=1}^{n} a_i b_i$ and $y = \sum_{i=1}^{m} c_i d_i$, where $a_i, c_i \in I$ and $b_i, d_i \in J$. Then

$$x - y = \sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{m} c_i d_i$$

which shows that $x - y \in IJ$. Also $rx = \sum_{i=1}^{n} (ra_i) b_i$, and since I is an ideal of R, we see that $ra_i \in I$ for all i. Therefore $rx \in IJ$ and we have proven that $IJ \lhd R$.

(b) Since $I \lhd R$, we have $IJ \subseteq I$. Similarly $IJ \subseteq J$ and we deduce that $IJ \subseteq I \cap J$.

(c) Since $I + J = R$, we may write $i + j = 1$ where $i \in I$ and $j \in J$. If $x \in I \cap J$, then $x = xi + xj \in JI + IJ = IJ$ (because R is commutative). Therefore $x \in IJ$ and we have proven that $I \cap J \subseteq IJ$. The result now follows from (b).

(d) Let $a \in R - 0$. We need to prove that a has a multiplicative inverse. Using $IJ \subseteq I \cap J$ with $I \cap J \subseteq aR$, we see that $aRaR \subseteq aR \subseteq aR$, hence $aras = a$ for some $r, s \in R$. Since $a \neq 0$ and R is an integral domain, we may cancel a to obtain $ars = 1$. We have now shown that all nonzero elements of R have a multiplicative inverse, hence R is a field.

2. (a) Since F is a finite Galois extension of K with Galois group S_5, there is a one-one correspondence between the fields strictly between F and K, and the proper nontrivial subgroups of S_5. Therefore we need to show that S_5 has more than 40 subgroups other than 1 and S_5. Now S_5 has 24 elements of order 5 which gives 6 subgroups of order 5; 20 elements of order 3 which gives 10 subgroups of order 3; 10 2-cycles which gives 10 subgroups of order 2; 15 permutations which are a product of two disjoint 2-cycles which gives 15 more subgroups of order 2; and now we have $6 + 10 + 10 + 15$ subgroups which is already more than 40, as required.

(b) The subfields E of F containing K which are Galois extensions of K correspond to the normal subgroups of $\mathrm{Gal}(F/K)$. Specifically if H is a normal subgroup of $\mathrm{Gal}(F/K)$, then the corresponding subfield is $\mathrm{Fix}(H)$, the elements of F which are fixed by all automorphisms of H. Furthermore we have $\mathrm{Gal}(\mathrm{Fix}(H)/K) \cong \mathrm{Gal}(F/K)/H$ and $\mathrm{Fix}(H) : K = \mathrm{Gal}(F/K) : H$. Since S_5 has a unique nontrivial normal subgroup, namely the alternating group A_5, it follows that the subfield E required is $\mathrm{Fix}(A_5)$. Then $E : K = 2$ and $\mathrm{Gal}(E/K) \cong S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$.

3. (a) $455 = 5 \cdot 7 \cdot 13$. We determine the number of Sylow 13-subgroups. This is congruent to 1 modulo 13 and divides 35. The only possibility is 1, which means that G has a normal subgroup A of order 13 and so G is not simple.

(b) Since G/A is a group of order 35, we can apply Sylow's theorems to see that G/A has exactly one subgroup of order 7, which by the subgroup correspondence theorem we may call H/A. Then $H/A \lhd G/A$, so $H \lhd G$. Now H is a group of order $|A| \cdot |H/A| = 13 \cdot 7$, and we may apply Sylow's theorems for the prime 7 to deduce that H has exactly one subgroup of order 7; we shall call this subgroup B. Then $B \lhd H$; in fact we can assert more, namely that $B \lhd G$. To see this, let $g \in G$. Then gBg^{-1} is a subgroup of $gHg^{-1} = H$ because $H \lhd G$, and since $|gBg^{-1}| = |B| = 7$, we see that $gBg^{-1} = B$ which establishes that $B \lhd G$. Similarly G has a normal subgroup of order 5, which we shall call C.

We now have that G has normal subgroups A, B, C of orders 13, 7 and 5 respectively. Since 13, 7 and 5 are coprime and their product is 455, we deduce that $G \cong A \times B \times C$. Let $a \in A$ be an element of order 13, let $b \in B$ be an element of order 7, and let $c \in C$ be an element of order 5. We want to show that abc is an element of order 455. Since the order of an element divides the order of the group, we certainly have the order of abc divides 455. Suppose the order of abc was less than 455. Then the order of abc would have to divide 455/13, or 455/7, or 455/5. Suppose the order of abc divided $455/13 = 35$. Then $(abc)^{35} = 1$ and since a, b, c commute, we see that $a^{35}b^{35}c^{35} = 1$. But $b^{35} = c^{35} = 1$, hence $a^{35} = 1$. This is not possible because a has order 13. Similarly the order of abc cannot divide 455/7 and 455/5. We deduce that abc has order 455, hence $\langle abc \rangle = G$ and the result is proven.

4. We shall use the fundamental theorem for finitely generated modules over a PID. Thus we may write

$$A \cong R^a \oplus \bigoplus_{i=1}^{m} (R/q_i R)^{a_i}$$
$$B \cong R^b \oplus \bigoplus_{i=1}^{m} (R/q_i R)^{b_i}$$

where a, b, a_i, b_i, m are nonnegative integers and the q_i are distinct prime powers. Since $A^n \cong B^n$, we have

$$R^{na} \oplus \bigoplus_{i=1}^{m} (R/q_i R)^{na_i} \cong R^{nb} \oplus \bigoplus_{i=1}^{m} (R/q_i R)^{nb_i}.$$

The fundamental theorem now gives that $na = nb$ and $na_i = nb_i$ for all i, hence $a = b$ and $a_i = b_i$ for all i and the result follows.

5. Since P is a projective module, it is a submodule of a free module F. The mapping $\theta: P \to F$ defined by $\theta p = 2p$ is a monomorphism, so by using the hypothesis that P is injective, we see that it has a left inverse $\phi: F \to P$. Since $\phi\theta$ is the identity mapping on P, we see that $p = 2\phi p$ for all $p \in P$ and hence $P = 2P$. Therefore $P = 2^n P$ and we deduce that $P = 2^n F$ for all positive integers n. But $\bigcap 2^n F = 0$ because F is a free module and the result follows. (Note: the hypothesis P is finitely generated has not been used.)

6. Let $\alpha: mB \to B$ denote the natural inclusion, and let $\beta: B \to B/mB$ denote the natural surjection. Then the exact sequence $mB \xrightarrow{\alpha} B \xrightarrow{\beta} B/mB \to 0$ yields an exact sequence

$$A \otimes mB \xrightarrow{1 \otimes \alpha} A \otimes B \xrightarrow{1 \otimes \beta} A \otimes B/mB \to 0$$

where 1 indicates the identity map. Therefore $A \otimes (B/mB) \cong (A \otimes B)/\mathrm{im}(1 \otimes \alpha)$, where im denotes the image of a map. Now $\mathrm{im}(1 \otimes \alpha)$ is the $\mathbb{Z}$-submodule of $A \otimes B$ generated by $\{a \otimes mb : a \in A \text{ and } b \in B\}$ and since $a \otimes mb = m(a \otimes b)$, this is the same as the $\mathbb{Z}$-submodule generated by $\{m(a \otimes b) : a \in A \text{ and } b \in B\}$. This submodule is precisely $m(A \otimes B)$, hence $\mathrm{im}(1 \otimes \alpha) = m(A \otimes B)$ and the proof is complete.

7. Let G be the group of order 588 and write 588 as a product of prime powers: $588 = 4 \cdot 3 \cdot 49$. The number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 12, hence there is a unique Sylow 7-subgroup A which must be normal in G. Since A has order 49, it is abelian and so certainly solvable. Thus we need only prove that G/A is solvable, because G/A and A solvable implies G solvable. Since G/A has order 12, this means we need to prove that all groups of order 12 are solvable.

   Let H be a group of order 12. The number of Sylow 3-subgroups is 1 or 4. Suppose there is exactly one Sylow 3-subgroup B. Then $B \lhd H$ and $H/B = 4$. Since groups of order 3 and 4 are abelian, we see that B and H/B are abelian and hence H is solvable. Suppose on the other hand that H has 4 Sylow 3-subgroups. If B_1 and B_2 are two distinct Sylow 3-subgroups, then $B_1 \cap B_2$ is a proper subgroup of B_1 whose order divides 3 by Lagrange's theorem, hence $B_1 \cap B_2 = 1$ and we conclude that H has (at least) 8 elements of order 3. Now the Sylow 2-subgroups of H have order 4, and every element of a Sylow 2-subgroup has order a power of 2. If H had more than one Sylow 2-subgroup, then H would have at least 5 elements of order a power of 2, consequently H would have at least $5 + 8 = 13$ elements, which is not possible because $|H| = 12$. Therefore H has a unique subgroup C of order 4, which must be normal in H. Since $|H/C| = 3$ and $|C| = 4$, we see that H/C and C are abelian, and we conclude that H is solvable. This completes the proof.

8. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Then clearly $K \subseteq L$. Also $(\sqrt{2}\sqrt{3})^3 - 9(\sqrt{2}\sqrt{3}) = 2\sqrt{2}$, hence $\sqrt{2} \in K$ and we deduce that $L = K$. Thus $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. It follows that K is the splitting field for the polynomial $(x^2-2)(x^2-3)(x^2-5)$ and we deduce that K is a Galois extension of $\mathbb{Q}$. In particular the number of fields between K and $\mathbb{Q}$ equals the number of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$.

   Now any element of $\mathrm{Gal}(K/\mathbb{Q})$ must send $\sqrt{2}$ to $\pm\sqrt{2}$, $\sqrt{3}$ to $\pm\sqrt{3}$, and $\sqrt{5}$ to $\pm\sqrt{5}$. It follows that every nonidentity element of $\mathrm{Gal}(K/\mathbb{Q})$ has order 2, and that $\mathrm{Gal}(K/\mathbb{Q})$ is elementary abelian of order 1,2,4 or 8.

   We shall use the following result: if a and b are products of distinct prime numbers and $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$, then $a = b$. To see this, write $\sqrt{a} = r + s\sqrt{b}$ where $r,s \in \mathbb{Q}$. Then $a = r^2 + 2rs\sqrt{b} + s^2 b$. Clearly $s \neq 0$ and $rs = 0$, consequently $r = 0$ and $a = s^2 b$ which establishes the result.

   It follows immediately that there are at least 8 subfields between $\mathbb{Q}$ and K, namely $\mathbb{Q}(\sqrt{2^c 3^d 5^e})$ where c,d,e are 0 or 1. Now if $|\mathrm{Gal}(K/\mathbb{Q})| > 8$, then there would be at most 5 subgroups of $\mathrm{Gal}(K/\mathbb{Q})$, consequently there would be at most 5 fields between K and $\mathbb{Q}$. This is a contradiction, so we must have $|\mathrm{Gal}(K/\mathbb{Q})| = 8$ and therefore $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

January 1998 Algebra Prelim Solutions

1. Let α be a root of f in K. Then $F(\alpha : F$ 1 because f has no roots in F, is less than 6 because f has degree 6, and divides 21. It follows that $F(\alpha : F$ 3. Let g be the minimum polynomial of α over F. Then g is an irreducible polynomial of degree 3 which divides f in $F\ X$, so we may write f gh in $F\ X$ where h has degree 3. Since h has no root in F, we see that h is irreducible in $F\ X$, so f gh is the factorization of f into irreducible polynomials in $F\ X$.

   Since f has at most two roots in K, we see that g and h have at most one root in K. It follows that we may write g g_1g_2 and h h_1h_2 where g_1, g_2, h_1, h_2 are irreducible in $K\ X$, g_1 and h_1 have degree 1, and g_2 and h_2 have degree 2. Then f $g_1g_2h_1h_2$ is the factorization of f into irreducible polynomials in $K\ X$.

2. The number of Sylow 59-subgroups divides 33 and is congruent to 1 modulo 59. Therefore there is only one Sylow 59-subgroup which means that G has a normal subgroup H of order 59.

   Now G/H is a group of order 33 and so the number of Sylow 3-subgroups of G/H is congruent to 1 modulo 3 and divides 11. Therefore G/H has a normal Sylow 3-subgroup, which we may write as A/H where A is a normal subgroup of G. Then A is a group of order 3*59 and the number of Sylow 3-subgroups of A is congruent to 1 modulo 3 and divides 59. Therefore A has a normal subgroup K of order 3. Observe that if g G, then gKg^{-1} is a subgroup of order 3 contained in gAg^{-1}. Since A is normal, gAg^{-1} A, so gKg^{-1} is a subgroup of order 3 in A and hence gKg^{-1} K, because A has exactly one subgroup of order 3. Therefore K is a normal subgroup of order 3 in G.

   Using exactly the same argument as above with the primes 3 and 11 interchanged, we see that G has a normal subgroup L of order 11. We have now proved that all the Sylow subgroups of G are normal, so G is isomorphic to a direct product of its Sylow subgroups. Also each nontrivial Sylow subgroup has prime order and is therefore cyclic. It follows that G abelian, and then by using the structure theorem for finitely generated abelian groups, we conclude that G is cyclic.

3. Since G is a nontrivial p-group, its center is nontrivial and therefore it has a central subgroup Z of order p. Then G/Z is a group of order p^{n-1} and since n 2, we see that G/Z is nontrivial p-group and hence it has a central subgroup of order p. We may write this subgroup as A/Z where A is a normal subgroup of G. Then A has order p^2 and since groups of order p^2 are abelian, it follows that A is a normal abelian subgroup of order p^2 as required.

4. The roots of X^3-2 are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ and it follows easily that K is the splitting field for X^3-2. Therefore $K/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$. Also $\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}$ 3 and $\mathbb{Q}(\sqrt[3]{2}$ K. Since the splitting field of a polynomial of degree 3 has degree dividing 6 and the Galois group is isomorphic to a subgroup of S_3, we conclude that $K : \mathbb{Q}$ 6 and the Galois group of K over $\mathbb{Q}$ is isomorphic to S_3.

5. (a) Obviously 0 A R. Let a, b A R. Then $a-b$ A and $a-b$ R, so $a-b$ A R. Finally let r R. Then ar A because A is an ideal of S, and ar R. Thus ar A R and we have proved that A R is an ideal of R.

(b) Let $x \in A$. Since F is the field of fractions of the PID R, we may write $x = ab^{-1}$ with $a, b \in R$ and $(a, b) = 1$. Then there exist $p, q \in R$ such that $ap + bq = 1$, so $px = q + b^{-1}$. Since $p, q, x \in S$, we see that $b^{-1} \in S$. Now A is an ideal of S, so $xb = a \in A \cap R = Rd$, so there exists $r \in R$ such that $xb = rd$. Then we have $x = b^{-1}rd \in Sd$ and the result follows.

6. (a) We have $|G/M : PM/M| = |G : PM|$ and $|G : P| = |G : PM||PM : P|$, so $|G/M : PM/M|$ divides $|G : P|$. Since P is a Sylow p-subgroup of G, we see that $|G : P|$ is prime to p and hence $|G/M : PM/M|$ is prime to p. This shows that PM/M is a Sylow p-subgroup of G.

(b) Let $n \in N$. Then $nPn^{-1} \subseteq P$ and $nMn^{-1} \subseteq M$, hence $nPMn^{-1} \subseteq PM$. This shows that Mn is in the normalizer of PM/M in G/M and we conclude that $n \in H$. The result follows.

(c) The number of Sylow p-subgroups of G/M is $|G/M : H/M| = |G : H|$, and the number of Sylow p-subgroups of G is $|G : N|$. Since $N \subseteq H$, we see that $|G : H|$ divides $|G : N|$ and the result follows.

7. (a) $A_5 \cong \mathbb{Z}/59\mathbb{Z}$.

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/885\mathbb{Z}$.

8. We shall use the structure theorem for finitely generated abelian groups. We may write

$$G \cong \mathbb{Z}^a \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$$
$$H \cong \mathbb{Z}^b \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{b_i}\mathbb{Z}$$

for certain integers a, b, a_i, b_i, n, and the p_i are distinct primes. Since $G \times G \cong H \times H$, we see that

$$\mathbb{Z}^{2a} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{2a_i}\mathbb{Z} \cong \mathbb{Z}^{2b} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{2b_i}\mathbb{Z}$$

Using the uniqueness statement in the structure theorem for finitely generated abelian groups, we see that $2a = 2b$ and $2a_i = 2b_i$ for all i. Therefore $a = b$ and $a_i = b_i$ for all i, which proves that $G \cong H$.

January 1999 Algebra Prelim Solutions

1. Let $0 \quad a \quad R$. We must prove that a is invertible, so suppose to the contrary that a is not invertible. Then a^2R is an ideal of R and since a is not invertible, we see that $aR \quad R$ and consequently $a^2R \quad R$. By hypothesis a^2R is a prime ideal of R and since $a^2 \quad a^2R$, we deduce that $a \quad a^2R$. Therefore $a \quad a^2r$ for some $r \quad R$. Since 0 is a prime ideal of R, we see that R is an integral domain and we deduce that $1 \quad ar$. Thus a is invertible and we have a contradiction. This completes the proof.

2. By hypothesis G has a normal subgroup of K of order p^3. Then G/K is a group of order q^3. A nontrivial q-group (where q is a prime) has a normal subgroup of order q, so G/K has a normal subgroup H/K of order q. Then H is a normal subgroup of order p^3q, as required.

3. Suppose R has an element a which is neither a zero divisor nor a unit. Then aR is a proper submodule of R, because a is not a unit. Also the map $r \quad ar$ is an R-map from R onto aR which has kernel 0, because a is a nonzero divisor. This shows that R is isomorphic to the proper R-submodule aR.

   Conversely suppose R is isomorphic to the proper R-sumodule M. Then there is an R-isomorphism $\theta\colon R \quad M$. Set $a \quad \theta 1$. Then $aR \quad (\theta 1\ R \quad \theta(1R \quad \theta R \quad M$, so $aR \quad R$ and we see that a is not a unit. Finally if $ar \quad 0$, then $\theta r \quad \theta(1r \quad (\theta 1\ r \quad ar \quad 0$ and we deduce that $r \quad 0$, because θ is an isomorphism. Therefore r is a nonzero divisor and the result follows.

4. Since α satisfies $X^2 - \alpha^2 \quad K(\alpha^2 \quad X$, we see that $K(\alpha : K(\alpha^2 \quad 1$ or 2. Also $K(\alpha : K \quad K(\alpha : K(\alpha^2 \quad K(\alpha^2 : K$. Since $K(\alpha : K$ is odd, we deduce that $K(\alpha : K(\alpha^2 \quad 1$ and the result follows.

5. By the fundamental structure theorem for finitely generated abelian groups, we know that G is a direct product of nontrivial cyclic p-groups. Since $x \quad G \quad x^p \quad 1$ has order p^2, we see that G is a direct product of exactly two nontrivial cyclic p-groups. It now follows that $G \quad \mathbb{Z}/p^5\mathbb{Z} \quad \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^4\mathbb{Z} \quad \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p^3\mathbb{Z} \quad \mathbb{Z}/p^3\mathbb{Z}$ (so there are three possible groups up to isomorphism).

6. Since K is a splitting over k, it can be written as $k(a_1, \ldots, a_n$ where $a_1, \ldots, a_n$ are all the roots of some polynomial $f \quad k\,X$. If $\sigma \quad \mathrm{Gal}(L/k$, then σa_i also satisfies f, because σ fixes all the coefficients of f, and so σ permutes the a_i. It follows that $\sigma K \quad k(\sigma a_1, \ldots, \sigma a_n \quad K$.

7. Let G be a simple group of order 280. The number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 40, so there are 1 or 8 Sylow 7-subgroups. There cannot be 1 Sylow 7-subgroup, because then the Sylow 7-subgroup would be normal which contradicts the hypothesis that G is simple. Therefore there are 8 Sylow 7-subgroups. Since two distinct Sylow 7-subgroups must have trivial intersection, we see that there are at least $8 \quad 6 \quad 48$ elements of order 7. The number of Sylow 5-subgroups is congruent to 1 modulo 5 and divides 56. There cannot be 1 Sylow 5-subgroup, for then it would be normal which would contradict the hypothesis that G is simple. Therefore there are 56 Sylow 5-subgroups. Since two distinct Sylow 5-subgroups must intersect in the identity, we see that there are at least $56 \quad 4 \quad 224$

elements of order 5. Finally since the Sylow 2-subgroup is not normal, there must be at least 9 elements whose order is a power of 2. We now count elements: we find that G has at least 48 224 9 281 elements, which is impossible because G has only 280 elements. Therefore no such G can exist and we deduce that there is no simple group of order 280.

8. Let K be a splitting field over F which contains E, let G Gal$(K/F$, and let H Gal$(K/E$. Since we are in characteristic zero, everything is separable and hence K is a Galois extension of F. Therefore by the fundamental theorem of Galois theory, we see that the number of fields between F and E is equal to the number of subgroups between G and H. Also $G:H$ n. By considering the permutation representation of G on the left cosets of H in G, we see that there is a normal subgroup N of G contained in H such that G/N $n!$. The number of subgroups between G and H is at most the number of subgroups between G and N, which is at most the number of subsets of G/N. Since the number of subsets of G/N is $2^{G/N}$, we deduce that the number of subfields between F and E is at most $2^{n!}$, as required.

August 1999 Algebra Prelim Solutions

1. We first factor 480 as 32 3 5. Note that since G is simple, it cannot have a nontrivial subgroup of index 7, because that would mean that G is isomorphic to a subgroup of A_7, which is not possible by Lagrange's theorem.

   (a) Let A P Q and suppose A 1. Since $P,Q \leqslant \mathbf{C}_G(A$, we see that P $\mathbf{C}_G(A$. Using Lagrange's theorem, we deduce that $\mathbf{C}_G(A$ 96, 160 or 480. We cannot have 480 because then A would be a central and hence a normal subgroup of G, which would contradict the hypothesis that G is simple. Also we cannot have $\mathbf{C}_G(A$ 96 or 160, because that would mean that G has a subgroup of index 5 or 3. We now have a contradiction, and we conclude that A 1.

   (b) The number of Sylow 2-subgroups is congruent to 1 modulo 2 and divides 15. It cannot be 1 because that would mean that G has a normal Sylow 2-subgroup. Nor can it be 3 or 5, because then G would have a subgroup of index 3 or 5. Therefore G has 15 Sylow 2-subgroups. Next the number of Sylow 3-subgroups is congruent to 1 modulo 3 and divides 96. This number cannot be 1, because that would mean that the Sylow 3-subgroup is normal. Nor can it be 4, because that would yield a subgroup of index 4. Therefore G has at least 10 Sylow 3-subgroups. Finally the number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 160. This number cannot be 1, because that would mean that the Sylow 7-subgroup is normal. Therefore G has at least 8 Sylow 7-subgroups.

   We now count elements. Since by (a) any two Sylow 2-subgroups intersect trivially, there are 15*31 nontrivial elements whose order is a power of 2. Next any two Sylow 3-subgroups intersect trivially, because a Sylow 3-subgroup has prime order 3, and we see that there are at least 10*2 elements of order 3. Finally any two Sylow 5-subgroups intersect trivially, because a Sylow 5-subgroup has prime order 5, and we deduce that G has at least 6*4 elements of order 5. We now count elements: we find that G has at least 15 31 10 2 6 4 509 nontrivial elements. Since G has only 480 elements altogether, we have now arrived at a contradiction. We conclude that there is no such group G.

2. Since R is a domain and $0 \not\in S$, we see that $S^{-1}R$ is a domain. Also for a,b R and s,t S, we have a/s b/t if and only if at bs. Suppose $p/1$ divides $(a/s\ (b/t$ in $S^{-1}R$. This means that there exists c/u $S^{-1}R$ such that $(p/1\ (c/u$ $(a/s\ (b/t$, which means that $pstc$ abu. Since p is prime, we see that p divides at least one of a,b,u. If p divides u, then $p/1$ is a unit in $S^{-1}R$ because $u/1$ is a unit in $S^{-1}R$. Therefore we may assume that p does not divide u; without loss of generality, we may assume that p divides a, say pq a. Then $(p/1\ (q/s$ a/s and we see that $p/1$ divides a/s. Therefore if $p/1$ is not a unit, it is prime and the result follows.

3. Let P be a finitely generated projective $k\,X\,/(X^3$ X -module. Then there is a $k\,X\,/(X^3$ X -module Q and an integer e such that P Q $(k\,X\,/(X^3$ X ^{e}. Note that X^3 X $X(X$ 1 ^{2} and $k\,X\,/(X^3$ X $k\,X\,/(X$ $k\,X\,/(X$ 1 ^{2}, so P Q $(k\,X\,/(X$ ^{e} $(k\,X\,/(X$ 1 ^{2} ^{e}. We may view this as an isomorphism of finitely generated $k\,X$ -modules. We use repeatedly without comment that a map between $k\,X\,/(X^3$ X -modules is an isomorphism as $k\,X\,/(X^3$ X -modules if and only if it is an isomorphism as $k\,X$ -modules. Since k is a field, $k\,X$ is a PID, so the structure theorem for finitely generated modules over a PID tells us that

$$P \quad \bigoplus_i k\,X\,/(f_i \quad \text{and} \quad Q \quad \bigoplus_i k\,X\,/(g_i$$

   where the f_i, g_i are either 0 or positive powers of monic irreducible polynomials. Then we have

$$\bigoplus_i k\,X\,/(f_i \quad \bigoplus_i k\,X\,/(g_i \quad (k\,X\,/(X^{\ e} \quad (k\,X\,/(X \quad 1^{\ 2^{\ e}}.$$

The uniqueness part of the structure theorem for finitely generated modules over a PID now tells us that $f_i \mid X$ or $(X \quad 1)^2$ for all i. It follows that a finitely generated $k[X]/(X^3 \quad X)$-module is isomorphic to a finite direct sum of modules of the form $k[X]/(X$ or $k[X]/(X^2 \quad 1)$.

4. Suppose there is a positive integer n such that $MJ^n \quad MJ^{n+1} \quad 0$. Then MJ^n is finitely generated because M is Noetherian, and $(MJ^n) J \quad MJ^{n+1} \quad MJ^n$. By Nakayama's lemma we deduce that $MJ^n \quad 0$, as required.

5. Since R is a right Artinian ring with no nonzero nilpotent ideals, the Wedderburn structure theorem tells us that $R \quad R_1 \quad \cdots \quad R_n$, where n is a positive integer, and the R_i are matrix rings over division rings. If $n \quad 1$, then $(1,0,\ldots,0)$ is a nontrivial idempotent, so $n \quad 1$ which means that R is a matrix ring over a division ring. If this matrix ring has degree $\quad 1$, then the matrix with 1 in the $(1,1)$ position and zeros elsewhere is a nontrivial idempotent. Therefore R is isomorphic to a matrix ring over a division ring, and the result follows.

6. The character table for S_4 is given below; the irreducible characters are $\chi_1,\ldots,\chi_5$. χ_1 is the principal character, χ_2 is the character coming from the sign of the permutation, ρ is the permutation character (not irreducible), $\chi_4 \quad \rho - \chi_1$, and $\chi_5 \quad \chi_2\chi_4$. The remaining row, the character of χ_3, can easily be filled in using the orthogonality relations.

Class Size	1	6	8	6	3
Class Rep	(1)	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	-1	0	1	-1
χ_5	3	1	0	-1	-1
ρ	4	2	1	0	0

7. Since splitting fields are determined up to isomorphism, we may as well assume that $K \quad$. Since the roots of $X^4 - 2$ are $\sqrt[4]{2}, \quad i\sqrt[4]{2}$, we see that $K \quad \mathbb{Q}(\sqrt[4]{2}, i)$. Now $X^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion for the prime 2, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \quad 4$. Also $i \notin \mathbb{Q}(\sqrt[4]{2})$ and i satisfies $X^2 \quad 1 \quad 0$, consequently $[K : \mathbb{Q}(\sqrt[4]{2})] \quad 2$. We deduce that $[K : \mathbb{Q}] \quad 8$ and therefore $|\mathrm{Gal}(K/\mathbb{Q})| \quad 8$. Now a group of order 8 has a normal subgroup of order 2 (a p-group has normal subgroups of any order dividing the order of the group); let H be a normal subgroup of order 2 in G, and let L be the fixed field of H. Then H has index 4 in G, so by the fundamental theorem of Galois theory, we see that L is a normal extension of degree 4 over $\mathbb{Q}$, as required.

Algebra Prelim Solutions, Summer 2002

1. (a) H acts on the set of conjugates of Q according to the formula $gQg^{-1} \mapsto hgQg^{-1}h^{-1}$ for $h \in H$ and $g \in G$. Note that $gQg^{-1} \leq G$ for all g, so O_Q is a set of subgroups. Let $S = \{h \in H \mid hQh^{-1} = Q\}$, the stabilizer of Q in H. Then $|O_Q||S| = |H|$. Now $h \in S$ if and only if $h \in H \cap \mathrm{N}_G(Q) = 1$, hence $|S| = 1$ and the result follows.

   (b) Let P be a Sylow p-subgroup of G. We apply the above with $H = P$. Since $P \cap \mathrm{N}_G(Q) = P \cap Q = 1$, we see that O_Q has $|P| = p^m$ subgroups. Furthermore all the subgroups of O_Q have prime order q, so any two of them must intersect in 1. Now each nonidentity element of a subgroup in O_Q has order q, consequently each subgroup of O_Q yields $q-1$ elements of order q and we deduce that G has at least $(q-1)p^m$ elements of order q. Therefore G has at most $pq^m - (q-1)p^m = p^m$ elements of order a power of p. Since $|P| = p^m$ and every element of a Sylow p-subgroup has order a power of p, we conclude that P is the only Sylow p-subgroup of G. Therefore P is normal in G and we are finished.

2. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $N = \mathrm{Gal}(K/F)$. Then $F \subseteq K$ and is the splitting field over $\mathbb{Q}$ for $(x^2-2)(x^2-3)$. Therefore N is a normal subgroup in $\mathrm{Gal}(K/\mathbb{Q})$ of index $[F : \mathbb{Q}]$. Now $\sqrt{2}$ satisfies $x^2 - 2$ and $\sqrt{2} \notin \mathbb{Q}$. Therefore $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   Next we show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then we could write $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, because every element of $\mathbb{Q}(\sqrt{2})$ can be written in this form. Squaring, we obtain $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Since $\sqrt{2} \notin \mathbb{Q}$, we deduce that a or $b = 0$. But $a = 0$ yields $\sqrt{3/2} \in \mathbb{Q}$, while $b = 0$ yields $\sqrt{3} \in \mathbb{Q}$, neither of which is true. We conclude that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Since $\sqrt{3}$ satisfies $x^2 - 3$, we deduce that $[F : \mathbb{Q}(\sqrt{2})] = 2$. Therefore

$$[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 * 2 = 4.$$

   Thus N is a normal subgroup of index 4 in $\mathrm{Gal}(K/\mathbb{Q})$.

   Suppose $\sqrt[8]{2} \in K$. Since $\sqrt[8]{2}$ satisfies $x^8 - 2$ and $x^8 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion for the prime 2, we see that 8 divides $[K : \mathbb{Q}]$, consequently 8 divides $|\mathrm{Gal}(K/\mathbb{Q})|$. But $|\mathrm{Gal}(K/\mathbb{Q})| = 4|N|$, so this is not possible if $|N|$ is odd.

3. (a) If X and Y are right R-modules and $\theta\colon X \to Y$ is an R-module homomorphism, then there is a unique group homomorphism $\theta \otimes 1\colon X \otimes_R C \to Y \otimes_R C$ such that $\theta(x \otimes c) = (\theta x) \otimes c$ for all $x \in X$ and $c \in C$.
First we apply this to the maps

$$(a,b) \mapsto a\colon A \oplus B \longrightarrow A$$
$$(a,b) \mapsto b\colon A \oplus B \longrightarrow B.$$

We obtain a group homomorphism

$$\theta\colon (A \oplus B) \otimes_R C \longrightarrow A \otimes_R C \oplus B \otimes_R C$$

such that $\theta((a,b) \otimes c) = (a \otimes c, b \otimes c)$. Next we apply it to the maps

$$a \mapsto (a,0) \otimes c\colon A \otimes_R C \longrightarrow (A \oplus B) \otimes_R C$$
$$a \mapsto (0,b) \otimes c\colon B \otimes_R C \longrightarrow (A \oplus B) \otimes_R C.$$

We obtain a group homomorphism

$$\phi\colon (A \otimes_R C) \oplus (B \otimes_R C) \longrightarrow (A \oplus B) \otimes_R C$$

such that $\phi(a \otimes c, b \otimes d) = (a,0) \otimes c + (0,b) \otimes d$.
Finally we show that $\phi\theta$ is the identity on $(A \oplus B) \otimes_R C$, and that $\theta\phi$ is the identity on $(A \otimes_R C) \oplus (B \otimes_R C)$. We have

$$\phi\theta(a,b) \otimes c = \phi(a \otimes c, b \otimes c) = (a,b) \otimes c.$$

Since $(A \oplus B) \otimes_R C$ is generated as an abelian group by elements of the form $(a,b) \otimes c$, we see that $\phi\theta$ is the identity. Also

$$\theta\phi(a \otimes c, b \otimes d) = \theta(a,0) \otimes c + \theta(0,b) \otimes d = (a \otimes c, b \otimes d).$$

Since $(A \otimes C) \oplus (B \otimes C)$ is generated as an abelian group by elements of the form $(a \otimes c, b \otimes d)$, we deduce that $\theta\phi$ is the identity. It now follows that $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$.

(b) Since M is a finitely generated $\mathbb{Z}$-module, we may express it as a finite direct sum of cyclic $\mathbb{Z}$-modules, say $M = \bigoplus_i \mathbb{Z}/a_i\mathbb{Z}$, where we may assume that $a_i \neq \pm 1$ for all i. Then by the first part, we see that

$$M \otimes_{\mathbb{Z}} M \cong \bigoplus_{i,j} \mathbb{Z}/a_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/a_j\mathbb{Z}.$$

Therefore it will be sufficient to prove $\mathbb{Z}/a_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/a_i\mathbb{Z} \neq 0$ for all i (of course even for just one i will be sufficient). However we can define a bilinear map

$$\theta\colon \mathbb{Z}/a_i\mathbb{Z} \times \mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/a_i\mathbb{Z}$$

by $\theta(x,y) = xy$. This induces a $\mathbb{Z}$-module homomorphism $\mathbb{Z}/a_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/a_i\mathbb{Z}$, which is obviously onto. We conclude that $\mathbb{Z}/a_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/a_i\mathbb{Z} \neq 0$, as required.

4. Note that $\mathrm{Ann}(m)$ is an ideal of R. Since R is Noetherian, we may choose $w \in M$ such that $\mathrm{Ann}(w)$ is maximal (that is $\mathrm{Ann}(w)$ is as large as possible, but not R). Suppose $\mathrm{Ann}(w)$ is not prime. Then there exists $a, b \in R \setminus \mathrm{Ann}(w)$ such that $ab \in \mathrm{Ann}(w)$, i.e. $abw = 0$. But then $a \in \mathrm{Ann}(bw)$ and $\mathrm{Ann}(w) \subseteq \mathrm{Ann}(bw)$. Furthermore $\mathrm{Ann}(bw) \neq R$ because $bw \neq 0$, so the maximality of $\mathrm{Ann}(w)$ has been contradicted and the result follows.

5. Suppose R is a field. Then an R-module is the same thing as an R-vector space, and since every vector space has a basis this means that every R-module is free; in particular every R-module is projective.

   Conversely suppose every R-module is projective. Since R is an integral domain, to prove R is a field we only need show that every nonzero element of R is invertible. Suppose to the contrary that x is a nonzero element of R which is not invertible. Then R/Rx is a nonzero R-module, so it has a nonzero element u. Note that $xu = 0$. Consider the exact sequence

   $$0 \longrightarrow Rx \longrightarrow R \longrightarrow R/xR \longrightarrow 0.$$

   Since R/xR is projective, the sequence splits, in particular R/xR is isomorphic to a submodule of R. Now R is an integral domain, so $xv \neq 0$ for all nonzero $v \in R$ and we deduce that $xu \neq 0$. We now have a contradiction and the result follows.

6. Since $Z_N = Z_{N+1}$, we see that $Z(G/Z_N) = 1$. Therefore $K \subseteq Z_N$.

   Now suppose L is a normal subgroup of G such that $Z(G/L) = 1$ and L does not contain Z_N. Then there is a nonnegative integer n such that

   $$Z_n \subseteq L, \quad Z_{n+1} \nsubseteq L.$$

   Choose $x \in Z_{n+1} \setminus L$. Then $xL \neq 1$ in G/L. Also $xgx^{-1}g^{-1} \in Z_{n+1}$ for all $g \in G$, because $xZ_{n+1} \in Z(G/Z_{n+1})$. Therefore $xgx^{-1}g^{-1} \in L$ and we deduce that $xL \in Z(G/L)$. This is a contradiction, and so the result is proven.

7. Let I be the set of matrices in $\mathrm{M}_2(\mathbb{Q}[x]/(x^2-1))$ of the form

$$\begin{pmatrix} a(x+1)+(x^2-1) & 0 \\ b(x+1)+(x^2-1) & 0 \end{pmatrix}.$$

with $a,b \in \mathbb{Q}$. Note that if $f \in \mathbb{Q}[x]$, then $(x-1)$ divides $f(x)-f(1)$, consequently $f(x)(x+1)+(x^2-1) = f(1)(x+1)+(x^2-1)$ in $\mathbb{Q}[x]/(x^2-1)$.

Now we verify that I is a left ideal of $\mathbb{Q}[x]/(x^2-1)$. Clearly I is an abelian group under addition. Since

$$\begin{pmatrix} f(x)+(x^2-1) & g(x)+(x^2-1) \\ h(x)+(x^2-1) & k(x)+(x^2-1) \end{pmatrix} \begin{pmatrix} a(x+1)+(x^2-1) & 0 \\ b(x+1)+(x^2-1) & 0 \end{pmatrix} = \begin{pmatrix} af(1)(x+1)+(x^2-1) & 0 \\ bh(1)(x+1)+(x^2-1) & 0 \end{pmatrix}$$

we see that I is closed under left multiplication by elements of $\mathbb{Q}[x]/(x^2-1)$, and it now follows that I is a left ideal.

Finally we need to show that I is a minimal ideal. Obviously $I \neq 0$ (note $x+1 \notin (x^2-1)$). Suppose J is a nonzero left ideal contained in I. We need to show that $J = I$. By multiplying on the left by the matrix

$$\begin{pmatrix} 0 & 1+(x^2-1) \\ 1+(x^2-1) & 0 \end{pmatrix}$$

if necessary, we may assume that I contains a matrix of the form

$$\begin{pmatrix} a(x+1)+(x^2-1) & 0 \\ b(x+1)+(x^2-1) & 0 \end{pmatrix}$$

with $a \neq 0$. Then by multiplying on the left by

$$\begin{pmatrix} c/a+(x^2-1) & 0 \\ d/a+(x^2-1) & 0 \end{pmatrix}$$

we see that J must be the whole of I and the result follows.

Algebra Prelim Solutions, Winter 2003

1. We have $f(x) = (x+1)(x^4+3)$; since $-1 \in \mathbb{Q}$, the splitting field for x^4+3 is also K. Let $\omega = (1+i)/\sqrt{2}$, a primitive 8th root of 1. Then $\omega^4 = -1$ and we see that the four roots of x^4+3 are $\omega^r \sqrt[4]{3}$ for $r = 1,3,5,7$. Therefore $K = \mathbb{Q}(\omega\sqrt[4]{3}, \omega^3\sqrt[4]{3}, \omega^5\sqrt[4]{3}, \omega^7\sqrt[4]{3})$. Since x^4+3 is irreducible by Eisenstein for the prime 3, we see that $[\mathbb{Q}(\omega\sqrt[4]{3}) : \mathbb{Q}] = 4$. Let γ denote complex conjugation. Since x^4+3 is a polynomial with real coefficients, we see that $\gamma \in \mathrm{Gal}(K/\mathbb{Q})$. Thus $\sqrt[4]{12} \in K$, because $\sqrt[4]{12} = \omega\sqrt[4]{3} + \gamma(\omega\sqrt[4]{3})$. Now $\sqrt[4]{12}$ satisfies $x^4 - 12$, which is irreducible by Eisenstein for the prime 3. Therefore $[\mathbb{Q}(\sqrt[4]{12}) : \mathbb{Q}] = 4$. Note that $\mathbb{Q}(\sqrt[4]{12}) \neq \mathbb{Q}(\omega\sqrt[4]{3})$, because the former is contained in $\mathbb{R}$ while the latter is not. We deduce that $K \neq \mathbb{Q}(\omega\sqrt[4]{3})$. Also $i = \omega^3\sqrt[4]{3}/\omega\sqrt[4]{3}$, which shows that $i \in K$. Since $\omega^{2r+1}\sqrt[4]{3} = i^r\omega\sqrt[4]{3}$, we conclude that $K = \mathbb{Q}(i, \omega\sqrt[4]{3})$. Therefore $[K : \mathbb{Q}(\omega\sqrt[4]{3})] = 2$ and hence $[K : \mathbb{Q}] = 8$.

   Of course a consequence of this is that x^4+3 remains irreducible over $\mathbb{Q}(i)$. Let $\theta \in \mathrm{Gal}(K/\mathbb{Q}(i))$ satisfy $\theta(\omega\sqrt[4]{3}) = \omega^3\sqrt[4]{3}$. Then $\theta(\omega^3\sqrt[4]{3}) = \omega^5\sqrt[4]{3}$, $\theta(\omega^5\sqrt[4]{3}) = \omega^7\sqrt[4]{3}$ and $\theta(\omega^7\sqrt[4]{3}) = \omega\sqrt[4]{3}$, in particular θ has order 4. Furthermore $\gamma\theta\gamma(i) = i$ and $\gamma\theta\gamma(\omega\sqrt[4]{3}) = \omega^7\sqrt[4]{3}$, which shows that $\gamma\theta\gamma = \theta^{-1}$. We now see that $\mathrm{Gal}(K/\mathbb{Q}) = \{\theta^r\gamma^s \mid r = 0,1,2,3,\ s = 0,1\}$ and is isomorphic to the dihedral group of order 8.

2. This is false. Consider the group $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, where $\mathbb{Z}_n$ denotes the integers modulo n. Then $(2,0)$ and $(0,1)$ both have order 2 (when we write $(2,0)$, the 2 means 2 modulo 4). Suppose θ is an automorphism such that $\theta(2,0) = (0,1)$. Then $2(\theta(1,0)) = \theta(2,0) = (0,1)$. On the other hand $2(\theta(1,0))$ is of the form $2(a,b) = (2a,0)$, and so cannot be equal to $(0,1)$. Thus we have a contradiction and we conclude that there is no such θ.

3. Let n denote the number of Sylow 2-subgroups. Since $2002 = 2 * 1001$, we see that a Sylow 2-subgroup has order 2 and $n \mid 1001$. Therefore each Sylow 2-subgroup has exactly one element of order 2 and n is odd. Also any element of order 2 is in exactly one Sylow 2-subgroup, consequently the number of elements of order 2 is n. Since the number of elements in the set $\{h \in H \mid h^2 = e\}$ is $n+1$ (the "+1" for the identity), we conclude that this number is even.

   However a better proof is to pair each $h \in H$ with h^{-1}. If $h^2 \neq e$, then $\{h, h^{-1}\}$ has order 2, otherwise $\{h, h^{-1}\}$ has order 1. It follows that the

number of elements $h \in H$ such that $h^2 \neq e$ has even order and since $|H|$ is even, it follows that the number of elements $h \in H$ such that $h^2 = e$ is even, as required.

4. Suppose G is nonabelian, so there exist $a, b \in G$ such that $ab \neq ba$. Set $g = aba^{-1}b^{-1}$, so $g \neq 1$. By hypothesis there exists $K \lhd G$ such that G/K is abelian and $g \notin K$. But $KaKb(Ka)^{-1}(Kb)^{-1} = Kg \neq 1$, which shows that $KaKb \neq KbKa$ and hence G/K is nonabelian, which is a contradiction. The result follows.

5. Certainly if A and B are commutative rings, then $A \times B$ is also a commutative ring. We need to show that if A and B are in addition Noetherian, then so is $A \times B$. Suppose $I_1, I_2, \ldots$ is an ascending chain of ideals in $A \times B$. Then $(0 \times B) \cap I_1, (0 \times B) \cap I_2, \ldots$ is an ascending chain of ideals in $0 \times B$. But $0 \times B \cong B$ and B is Noetherian, hence there exists a positive integer M such that $0 \times B \cap I_n = 0 \times B \cap I_M$ for all $n \geq M$. Also $(A \times B)/(0 \times B) \cong A$ as rings, so $(A \times B)/(0 \times B)$ is Noetherian. Therefore the ascending chain of ideals $(0 \times B) + I_1, (0 \times B) + I_2, \ldots$ of $(A \times B)/(0 \times B)$ becomes stationary, that is there is a positive integer N such that $(0 \times B) + I_n = (0 \times B) + I_N$ for all $n \geq N$. Let P be the maximum of M and N. We claim that $I_n = I_P$ for all $n \geq P$. Obviously $I_n \supseteq I_P$ for all $n \geq P$, so we need to show the reverse inclusion. Let $x \in I_n$. Since $(0 \times B) + I_n = (0 \times B) + I_P$, we may write $x = b + i$ where $b \in 0 \times B$ and $i \in I_P$. Since $x, i \in I_n$, we see that $b \in (0 \times B) \cap I_n$ and hence $b \in (0 \times B) \cap I_P$, because $(0 \times B) \cap I_n = (0 \times B) \cap I_P$. This shows that $x \in I_P$ and hence $I_n = I_P$ for $n \geq P$.

6. Obviously P/IP is an R/I-module; we need to prove that it is projective. Suppose we are given an R/I-epimorphism $\mu : M \twoheadrightarrow N$ of R/I-modules and an R/I-map $\theta : P/IP \to N$. We need an R/I-map $\beta : P/IP \to M$ such that $\theta = \mu\beta$. Let $\pi : P \to P/IP$ denote the natural epimorphism. We can also view M and N as R-modules, and then μ is also an R-map. Since P is a projective R-module, certainly there exists an R-map $\alpha : P \to M$ such that $\mu\alpha = \theta\pi$. If $i \in I$ and $p \in P$, then $\alpha(ip) = i\alpha p \in IM = 0$. Therefore $IP \subseteq \ker\alpha$ and we deduce that α induces an R/I-map $\beta : P/IP \to M$ satisfying $\beta\pi = \alpha$. Then $\mu\beta\pi = \mu\alpha = \theta\pi$ and since π is onto, we conclude that $\mu\beta = \theta$.

   Sketch of alternate proof. Since P is projective, we may write $P \oplus Q \cong F$ for some R-modules Q, F with F free. Then $P/IP \oplus Q/IQ \cong F/IF$ and since F/IF is a free R/IR-module, we see that P/IP is a projective R/IR-module.

7. (a) Certainly $k+I$ is a subgroup of $k[x]$ under addition; we need to show that it is closed under multiplication. However if $a,b \in k$ and $i,j \in I$, then $(a+i)(b+j) = ab+(aj+ib+ij) \in k+I$, because $aj, ib, ij \in I$ by using $I \lhd k[x]$.

   (b) Let $R = k+I$. We first prove that $k[x]$ is finitely generated as an R-module. We may write $I = (f)$ where f is a monic polynomial in $k[x]$. Let d denote the degree of f and set $M = R + Rx + \cdots + Rx^d$, an R-submodule of $k[x]$. We prove by induction on n that $x^n \in M$ for all $n \geq 0$. This is obviously true if $n = 0$, because $1 \in R$. It is also obviously true for $d = 0$ because then $R = k[x]$. Now suppose $d, n > 0$. Then by the division algorithm $x^n = qf + r$, where $q, r \in k[x]$ and $\deg r < n$. Then we must have $\deg q < n$. Therefore by induction $q, r \in M$, and it follows that $x^n \in M$ as required.

   Now $k[x] \otimes_R k[x]/I$ is an R-module and also an R/I-module. Since $k[x]$ is a finitely generated R-module, we see that $k[x]/I$ is also a finitely generated R-module, and we deduce that $k[x] \otimes_R k[x]/I$ is a finitely generated R/I-module. Since $R/I = (k+I)/I \cong k/k \cap I = k/0 \cong k$, we conclude that $k[x] \otimes_R k[x]/I$ is a finitely generated k-module and the result follows.

Algebra Prelim Solutions, Fall 2005

1. Let G be a group of order 18. The number of Sylow 3-subgroups is congruent to 1 mod 3 and divides $18/9 = 2$. Therefore G has a unique Sylow 3-subgroup H of order 9, and $H \lhd G$. Also G has an element x of order 2. Then $G \cong H \rtimes \langle x \rangle$. Since groups of order p^2 are prime, H is an abelian group. For a positive integer n, let C_n denote the cyclic group of order n. We have three cases to consider.

   (a) The conjugation action of x on H is trivial, that is $xhx^{-1} = h$ for all $h \in H$ and we have $G \cong H \times \langle x \rangle$. There are two isomorphism classes for H, namely C_9 and $C_3 \times C_3$. It follows that there are two isomorphism classes for G in this case.

   (b) The conjugation action of x on H is nontrivial and $H \cong C_9$. There is exactly one automorphism of H of order two, namely $h \mapsto h^{-1}$ for $h \in H$. It follows that there is exactly one isomorphism class for G in this case.

   (c) The conjugation action of x on H is nontrivial and $H \cong C_3 \times C_3$. Either x acts by inversion on H and this gives us one isomorphism class for G. Otherwise we may write $H = A \times B$ where $A, B \cong C_3$, x centralizes A and x acts by inversion on B. This yields a second isomorphism class for G.

   We conclude that there are $2 + 1 + 2 = 5$ isomorphism classes for a group of order 18.

2. First suppose that A is Noetherian. Then $A[X,Y]$ is Noetherian by Hilbert's basis theorem. Since factor rings of Noetherian rings are Noetherian, we see that $A[X,Y]/(X^2 - Y^2)$ is also Noetherian.

   Conversely suppose $A[X,Y]/(X^2 - Y^2)$ is Noetherian. Since $(X,Y) \supset (X^2 - Y^2)$, we see that $A[X,Y]/(X,Y)$ is also Noetherian. But $A[X,Y]/(X,Y) \cong A$, because the homomorphism

   $$X \mapsto 0,\ Y \mapsto 0 \colon A[X,Y] \to A$$

   is surjective with kernel (X,Y), and the result follows.

3. Let $0 \neq u \in F^2$ and let S denote the stabilizer in $\mathrm{GL}_n(F)$ of the one-dimensional subspace Fu. We need to prove that S is not simple. Set $D = \{\mathrm{diag}(f, f) \mid$

$0 \neq f \in F\}$, where $\mathrm{diag}(f,f)$ indicates the invertible matrix in $\mathrm{GL}_2(F)$ which has f's on the main diagonal and zeros elsewhere. Then D is a central subgroup of S and since $|F| \geq 3$, it is not 1. Let v be an element of F^2 which is not in Fu. Then $\{u,v\}$ is a basis of F^2 and so we can define a linear isomorphism of F^2 by $u \mapsto u$, $v \mapsto u+v$. This yields an element of $S \setminus D$. Thus D is a normal subgroup of S which is neither 1 nor D, and we conclude that S is not simple.

4. Clearly M cannot be free of rank 0. Nor can M be free of rank at least 2, because if $a,b \in M$ were part of a free R-basis for M, we would have $0 \neq ab \in aR \cap bR$, which would mean that $\{a,b\}$ was not linearly independent over R. Therefore the only possibility of M being free is that it is free of rank 1. This means we can write $2R + XR = cR$ for some $c \in R$. There are several methods to show that this is not possible; we present one of them.

   Since $2 \in cR$, we see that c is a polynomial of degree zero and thus $c = \pm 1$ or ± 2. Without loss of generality, we may assume that $c = 1$ or 2. Since $X \in cR$, we may write $X = cf$ for some polynomial $f \in \mathbb{Z}[X]$. By considering the leading coefficient (degree 1) of f, we see that $c = 1$ and we deduce that there exist $g,h \in R$ such that $2g + Xh = 1$. This is not possible because the left hand side has constant coefficient $\in 2\mathbb{Z}$ and in particular cannot be 1. It follows that M is not a free R-module.

5. Since $\sigma a - a \in F$ for all $\sigma \in G$, we see that $(\sum_{\sigma \in G} \sigma a) - |G|a \in F$. Now $\tau \sum_{\sigma \in G} \sigma a = \sum_{\sigma \in G} \sigma a$ for all $\tau \in G$. Since K/F is a Galois extension with Galois group G, it follows that $\sum_{\sigma \in G} \sigma a \in F$ and we deduce that $|G|a \in F$. We conclude that $a \in F$ because F has characteristic zero.

6. Set $m = \sqrt{n}$. A finite dimensional simple algebra over an algebraically closed field is isomorphic to a full matrix ring over the field. In this situation, this means S is isomorphic to $\mathrm{M}_m(\mathbb{C})$, the $m \times m$ matrices over $\mathbb{C}$. Let e_{ij} $(1 \leq i,j \leq m)$ denote the matrix units of $\mathrm{M}_m(\mathbb{C})$, so e_{ij} has 1 in the (i,j)th position and zeros elsewhere. Then Se_{ii} is the ith column of S and we see that $S = Se_{11} \oplus Se_{22} \oplus \cdots \oplus Se_{mm}$. All that remains to prove is that Se_{ii} is irreducible for all i. Without loss of generality, we may assume that $i = 1$. Suppose M is a nonzero R-submodule of Se_{11}. The general element α of Se_{11} is of the form $\sum_i a_i e_{i1}$. If this is a nonzero element of M, then $a_i \neq 0$ for some i, $1 \leq i \leq m$, and we deduce that $e_{11} = a_i^{-1} e_{1i} \alpha \in M$. Thus $M = Se_{11}$ and the result follows.

7. The map $f \mapsto f \otimes 1 \colon \overline{F} \to \overline{F} \otimes_F L$ is an algebra monomorphism with image $\overline{F} \otimes 1$. Furthermore, if $\{\lambda_1, \ldots, \lambda_n\}$ is a basis for L over F, then $\{1 \otimes \lambda_1, \ldots, 1 \otimes \lambda_n\}$ is a basis for $\overline{F} \otimes_F L$ over $\overline{F} \otimes 1$. It follows that $\overline{F} \otimes_F L$ is a field extension of degree n over $\overline{F}$ and since $\overline{F}$ is algebraically closed, we deduce that $n = 1$. Therefore $L = F$ as required.

Algebra Prelim Solutions, Fall 2007

1. Let G be a simple group of order 168. The number of Sylow 7-subgroups of G is congruent to 1 mod 7 and divides $168/7 = 24$. This number cannot be 1 because that would mean that G has exactly one Sylow 7-subgroup, consequently G would have a normal Sylow 7-subgroup and we would deduce that G is not simple, contrary to the hypothesis. It follows that G has exactly 8 Sylow 7-subgroups. Also by Lagrange's theorem, two distinct Sylow 7-subgroups must intersect in the identity. Since any element of order 7 is contained in a Sylow 7-subgroup and there are 6 elements of order 7 in each Sylow 7-subgroup, we deduce that there are $8 * 6 = 48$ elements of order 7 in G.

2. Note that $\rho = i$. The following are easy to check: $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}\sqrt{3}$. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a Galois extension of degree 4 over $\mathbb{Q}$. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$ and let L be the splitting field of $x^2 - 3$ over $\mathbb{Q}$. The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$, hence K is a Galois extension of degree 8 over $\mathbb{Q}$, and has maximal real subfield of degree 4 over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt[4]{2})$. Since this subfield is not normal over $\mathbb{Q}$, we deduce that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is not contained in K. Therefore $K \cap L = \mathbb{Q}$, and we deduce that $K \cap L(i) = \mathbb{Q}(i)$. The Galois group of $L/\mathbb{Q}$ has order two and is therefore isomorphic $\mathbb{Z}/2\mathbb{Z}$. Also the Galois group of $K/\mathbb{Q}$ is a group of order 8 and not every subgroup is normal, because $\mathbb{Q}(\sqrt[4]{2})$ is not normal over $\mathbb{Q}$. and we deduce that this group is isomorphic to the dihedral group D_8 of order 8. Finally $\mathrm{Gal}(K/\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z}$, being generated by the automorphism determined by $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$.

   (a) The Galois group of $(x^4-2)(x^2-3)$ over $\mathbb{Q}$ is $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong D_8 \times \mathbb{Z}/2\mathbb{Z}$. The Galois group of $(x^4-2)(x^2-3)$ over $\mathbb{Q}(i)$ is $\mathrm{Gal}(K/\mathbb{Q}(i)) \times \mathrm{Gal}(L(i)/\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   (b) $\mathbb{Q}(i)$ is Galois over $\mathbb{Q}$ because it is the splitting field of $x^2 + 1$ over $\mathbb{Q}$.

   (c) Yes, because $\mathrm{Gal}(LK/\mathbb{Q}(i))$ has nontrivial normal subgroups.

3. Since $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split exact, there exists $h\colon B \to A$ such that $hf = 1_A$, the identity map on A. Then $(1_D \otimes h)(1_D \otimes f) = 1_D \otimes hf = 1_D \otimes 1_A = 1$. Thus if $x \in D \otimes_R A$ and $(1_D \otimes f)(x) = 0$, then $(1_D \otimes f)(1_D \otimes h)(x) = 0$, consequently $1(x) = 0$ and we conclude that $x = 0$, as required.

4. Certainly $S^{-1}R$ is an integral domain, since it is a subring of the field of fractions of R, so we need to prove that every ideal of $S^{-1}R$ is principal. Let $I \lhd S^{-1}R$ and let $J = I \cap R$. Then $J \lhd R$, so $J = xR$ for some $x \in R$. Obviously $xS^{-1}R \subseteq I$, so it remains to prove that $xS^{-1}R \supseteq I$. However if $y \in I$, then $sy \in I \cap R = J$ where $s \in S$ and hence we may write $sy = xr$ for some $r \in R$. Therefore $y = s^{-1}(sy) = xs^{-1}r \in xS^{-1}R$ and the result is proven.

5. Let G be a group of order $2^4 \cdot 11^2$. The number of Sylow 11-subgroups is congruent to 1 mod 11 and divides 16, consequently there is exactly one Sylow 11-subgroup; call this Sylow 11-subgroup H. Then $H \lhd G$. Now G/H and H are p-groups for $p = 2$ and 11 respectively, and p-groups are solvable (even nilpotent). However the property of being solvable is closed under extensions, that is H and G/H solvable implies G is solvable, which is the required result.

6. (a) Apply Eisenstein's criterion for the prime 3.

   (b) We know that f is irreducible (from (a)) and that g is irreducible (use Eisenstein for the prime 2). Since $\mathbb{Q}[x]$ is a PID, we see that (f) and (g) are maximal ideals of $\mathbb{Q}[x]$. Furthermore $(f) \neq (g)$, because f and g are not scalar multiples of each other. It now follows from the Chinese remainder theorem that $\mathbb{Q}[x]/(fg) \cong \mathbb{Q}[x]/(f) \times \mathbb{Q}[x]/(g)$, a product of two fields. The dimension over $\mathbb{Q}$ of these two fields are the degrees of the polynomials f and g, that is 4 and 2 respectively.

7. (a) Since $1 \cdot 0 = 0$, we see that $0 \in t(X)$. Next suppose that $x, y \in t(X)$. Then there exist $r, s \in R \setminus 0$ such that $rx = 0 = sy$ and we have $(rs)(x+y) = 0$. Since $rs \neq 0$ because R is an integral domain, we conclude that $x + y \in t(X)$. Finally suppose that $x \in t(X)$ and $r \in R$. Then there exists $s \in R \setminus 0$ such that $sx = 0$ and consequently $s(rx) = 0$. This shows that $rx \in t(X)$ and we have established that $t(X)$ is an R-submodule of X.

   (b) Write $T = t(X)$ and let $x \in t(T)$; we want to prove that $x \in T$. Since $x \in t(T)$, there exists $s \in R \setminus 0$ such that $sx \in T$, and then there exists $t \in R \setminus 0$ such that $t(sx) = 0$. It follows that $(st)x = 0$ and since $st \neq 0$ because R is an integral domain, we conclude that $x \in T$ as required.

   (c) Because $t(X/t(X))$ is cyclic, $t(X/t(X)) \cong R/I$ for some $I \lhd R$. But $t(X/t(X)) = 0$ by (b), hence $I = 0$ and we deduce that $X/t(X) \cong R$. Since R is a projective R-module, $0 \to t(X) \to X \to X/t(X) \to 0$ splits, in particular $X \cong t(X) \oplus R$, as required.

Algebra Prelim Solutions, December 2007

1. (a) By using the elementary divisor decomposition, up to isomorphism, there are three abelian groups of order p^3q, namely $\mathbb{Z}_{p^3} \times \mathbb{Z}_q$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_q$, and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$.

   (b) The first group above is generated by one element, while the third requires 3 elements. Therefore $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{pq}$, because $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, as required.

2. We have $[k(\alpha) : k] = \deg f$ and $[K : k(\alpha)][k(\alpha); k] = [K : k]$. Thus $\deg f \mid [K : k]$ and the result follows.

3. By Gauss's lemma, f is irreducible in $Q[x]$. Since $Q[x]$ is a PID, this tells us that $fQ[x]$ is a maximal ideal of $Q[x]$. The result follows.

4. A_4 is a normal subgroups of S_4 and $V := \{(1), (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4 (even normal in S_4). Since $|S_4/A_4| = 2$, $|A_4|/V = 3$, $|V| = 4$, the groups S_4/A_4, A_4/V and V are all abelian, because groups of order 2,3 or 4 are abelian. This proves that S_4 is solvable.

5. We have a short exact sequence $0 \to \ker f \to P \xrightarrow{f} Q \to 0$. Since Q is projective, the sequence splits, so $P \cong Q \oplus \ker f$. This proves the result, because direct summands of projective modules are projective.

6. First observe that $Q \otimes_R Q \cong Q$ as Q-modules. To do this, define $f\colon Q \times Q \to Q$ by $f(p,q) = pq$. Clearly this is R-bilinear, so induces an R-map $g\colon Q \otimes_R Q \to Q$ satisfying $g(p \otimes q) = pq$. Also we can define a Q-map $h\colon Q \to Q \otimes_R Q$ by $h(q) = q \otimes 1$. Since $gh(q) = g(q \otimes 1) = q$, we see that gh is the identity on Q. Now consider $hg(p \otimes q) = pq \otimes 1$. Write $q = a/b$ where $a, b \in R$ with $b \neq 0$. Then $pq \otimes 1 = pa/b \otimes 1 = p/b \otimes ab/b = pb/b \otimes a/b = p \otimes q$ and it follows that hg is the identity on $P \otimes Q$, because we only need to check that hg is the identity on the "simple tensors". Thus h is one-to-one and onto, and our observation is established.

   Now observe that $Q \otimes_Q V \cong V$. Indeed we can define a Q-bilinear map $\theta\colon Q \times V \to V$ by $\theta(q,v) = qv$, and this induces a Q-map $\phi\colon Q \otimes_Q V \to V$ satisfying $\phi(q \otimes v) = qv$. Also we can define a Q-map $\psi\colon V \to Q \otimes_Q V$ by $\psi(v) = 1 \otimes v$. Then $\phi\psi(v) = \phi(1 \otimes v) = v$, so $\phi\psi$ is the identity on V. Since $\psi\phi(q \otimes v) = \psi(qv) = 1 \otimes qv = q \otimes v$ and $\psi\phi$ is the identity on $Q \otimes_Q V$

provided it is the identity on the simple tensors, we see that $\psi\phi$ is the identity on $Q \otimes_Q V$, and the result follows.

Note that this proof does not use the hypothesis that V is finite dimensional.

7. Let G denote the Galois group of F over K. Since G is a p-group for the prime $p = 11$, it has a sequence of normal subgroups $1 = G_4 \lhd G_3 \lhd G_2 \lhd G_1 \lhd G_0 = G$, such that $G_i \lhd G$ and $|G_{i+1}/G_i| = 11$ for all i. Now let K_i be the fixed subfield of G_i in K, for $i = 0, 1, \ldots, 4$. Then K_i is a Galois extension of F for all i, because $G_i \lhd G$. Since $[K_i : K_{i-1}] = |G_{i-1}/G_i| = 11$, the result is proven.

8. Suppose R/I is a projective R-module. Then we may write $R = I \oplus J$ for some R-submodule J of R. Of course R-submodules of R are the same as ideals, so J is an ideal of R. Since M is the unique maximal ideal of R and $I \subseteq M$, we must have $J = R$. But then $J \supseteq I$ and thus $I + J$ is not a direct sum. We now have a contradiction and the result follows.

Algebra Prelim Solutions, August 2009

1. Let $s \in S$ and let H denote the stabilizer of s in G. Since G acts transitively on S, we have $|G| = p^n|H|$, hence $p^n \mid |G|/|P \cap H|$ and we deduce that $p^n \mid |P|/|P \cap H$, because $p \nmid |G|/|P|$. Therefore p^n divides the size of the orbit of s under P, because $P \cap H$ is the stabilizer of s in P. Thus we must have the orbit of s under P is the whole of S and the result is proven.

2. Let G be a simple group of order 448. The number of Sylow 2-subgroups of G is congruent to 1 mod 2 and divides 7, and cannot be 1 because G is not simple. Therefore G has exactly 7 Sylow 2-subgroups and because G is simple, we deduce that G is isomorphic to a subgroup of A_7. This is not possible because 448 does not divide $|A_7|$, so the result is proven.

3. (a) If x^2+1 was not irreducible, then it would have a root in $\mathbb{Z}/3\mathbb{Z}$. This is not the case, because $x^2 = 0$ or $1 \mod 3$.

   (b) We have an epimorphism $\mathbb{Z}/3\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[i]/3\mathbb{Z}[i]$ determined by $x \mapsto i$ whose kernel contains x^2+1. Thus from part (a), we see that $\mathbb{Z}[i]/3\mathbb{Z}[i]$ is a field and hence 3 is a prime in $\mathbb{Z}[i]$. We can now apply Eisenstein's criterion for the prime 3. Since 3 divides 3 and -9, but 3^2 does not divide 12 in $\mathbb{Z}[i]$, the result is proven.

4. By the structure theorem for finitely generated modules over a PID, there is an R-submodule K of M containing N such that M/K is a torsion module and K/N is a free module, so there exists $0 \neq r \in R$ such that $Mr \subseteq K$. Since K/N is free, there exists a submodule L of K such that $L+N = K$ and $L \cap N = 0$. The result follows.

5. Let $b \in B$. Since f is onto, there exists $a \in A$ such that $f(a) = b$. Now set $k(b) = g(a)$. If we had instead chosen $a' \in A$ such that $f(a') = b$, then

$$jg(a') = hf(a') = h(b) = hf(a) = jg(a)$$

   and we deduce that $g(a') = g(a)$ because j is one-to-one; in other words, the definition of k does not depend on the choice of a. Next we need to show that k is an R-module homomorphism. Suppose $b, b' \in B$ and choose $a, a' \in A$ such that $f(a) = b$ and $f(a') = b'$. Then $f(a+a') = b+b'$. Thus $k(b+b') = g(a+a') = g(a) + g(a') = k(b) + k(b')$. Also if $r \in R$, then $f(ar) = br$, consequently $k(br) = g(ar) = g(a)r = k(b)r$ and we have shown that k is

an R-module homomorphism. Clearly $kf = g$. Furthermore $jkf = jg = hf$ and since f is onto, we deduce that $jk = h$. Finally k is unique because j is one-to-one.

6. Solving $x^4 - 2x^2 + 9 = 0$, we find that $x^2 = 1 \pm 2\sqrt{2}i$ and we deduce that the roots of $x^4 - 2x^2 + 9$ are $\pm\sqrt{2} \pm i$. It follows that the splitting field is $\mathbb{Q}[i, \sqrt{2}]$. Since this has degree 4 over $\mathbb{Q}$, we see that the Galois group has order 4. The automorphisms induced by $i \mapsto -i$, $\sqrt{2} \mapsto \sqrt{2}$ and $i \mapsto i$, $\sqrt{2} \mapsto -\sqrt{2}$ both have order 2 and we conclude that the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

7. We can define an R-bilinear map $R/I \times R/J \to R/(I+J)$ by $(r+I, s+J) \mapsto rs$. This induces an R-module map $\theta\colon R/I \otimes_R R/J \to R/(I+J)$ satisfying $\theta((r+I) \otimes (s+J)) = rs + I + J$. Now define $\phi\colon R \to R/I \otimes_R R/J$ by $\phi(r) = (r+I) \otimes_R (1+J)$. Then ϕ is an R-module map and clearly $I \subseteq \ker\phi$. Also if $j \in J$, then $\phi(j) = (j+I) \otimes (1+J) = (1+I) \otimes (j+J) = 0$. It follows that $I + J \subseteq \ker\phi$ and we deduce that ϕ induces an R-module map $\psi\colon R/(I+J) \to R/I \otimes_R R/J$ such that $\psi(r+I+J) = (r+I) \otimes (1+J)$. Note that $\theta\psi(r + I + J) = \theta((r+I) \otimes (1+J)) = r + I + J$ so $\theta\psi$ is the identity map. Finally $\psi\theta(r+I) \otimes (s+J) = \psi(rs+I+J) = (rs+I) \otimes (1+J) = (r+I) \otimes (s+J)$ and we conclude that $\psi\theta$ is also the identity map. This shows that θ and ψ are isomorphisms, and the result is proven.

Algebra Prelim Solutions, August 2011

1. First we write 380 as a product of prime powers, namely $2^2 * 5 * 19$. Suppose by way of contradiction G is a simple group of order 380. The number of Sylow 19-subgroups is congruent to 1 mod 19 and divides 20, hence is 1 or 20. But 1 is ruled out because then G would have a normal subgroup of order 19, which would contradict the hypothesis that G is simple. Therefore G has 20 Sylow 19-subgroups. Next we consider the Sylow 5-subgroups. The number is congruent to 1 mod 5 and divides $4 * 19$. Thus there are 1 or 76 Sylow 5-subgroups.

   Now we count elements. If P and Q are distinct Sylow 19-subgroups, then $P \cap Q \neq P$ and $P \cap Q \leqslant P$. Since $|P \cap Q|$ divides $|P| = 19$ by Lagrange's theorem, we deduce that $P \cap Q = 1$. It follows that G has at least $20 * 18 = 360$ elements of order 19. Similarly two distinct Sylow 5-subgroups intersect trivially and we deduce that G has at least $76 * 4 = 304$ elements of order 5. We conclude that G has at least $360 + 304 = 664 > 380$ elements, which is a contradiction. Therefore there is no simple group of order 380.

2. Let $\omega = \bar{2} \in \mathbb{F}_7$, so $\omega \neq 1 = \omega^3$. We have $(f-g)(f-\omega g)(f-\omega^2) = h^3$. Since f, g are coprime, we see that $f-g$, $f-\omega g$, $f-\omega^2 g$ are pairwise coprime. Now use the fact that $k[x_1, \ldots, x_n]$ is a UFD; remember that the units of $k[x_1, \ldots, x_n]$ are precisely the nonzero elements of k. Write $h = up_1^{r_1} \ldots p_m^{r_m}$ where $0 \neq u \in k$, m is a nonnegative integer, p_i is prime for all i, and r_i is a positive integer for all i. Since $f-g$, $f-\omega g$, $f-\omega^2 g$ are pairwise coprime, we see that if p_i divides one of these three polynomials, then p_i doesn't divide the other two polynomials, and it follows that $p_i^{3r_i}$ is the precise power of p_i which divides this polynomial. We deduce that each of $f-g$, $f-\omega g$, $f-\omega^2 g$ is of the form uq^3 for some unit u and some polynomial q, and the result follows.

3. We use the structure theorem for finitely generated modules over a PID, elementary divisor form. We may write $M = \bigoplus_{i \in I} (R/p^i R)^{e_i} \oplus \bigoplus_i C_i$, where $e_i \in \mathbb{N}$, I is a finite subset of $\mathbb{N}$, and the C_i are modules of the form R or $R/q^h R$, where $h \in \mathbb{N}$ and q is a prime which is not associate to p. This expresses M in a unique way as a direct sum of indecomposable R-modules. The hypothesis that $pm = 0 \neq m$ implies Rm is not a direct summand of M tells us that $1 \notin I$. Similarly we may write $N = \bigoplus_{i \in J} (R/p^i R)^{f_i} \oplus \bigoplus_i D_i$, where $f_i \in \mathbb{N}$, J is a finite subset of $\mathbb{N}$ not containing 1, and the D_i are

modules of the form R or R/q^fR, where $f \in \mathbb{N}$ and q is a prime which is not associate to p. Note that $pC_i \cong C_i$ and $pD_i \cong D_i$ for all i. Also $p(R/p^iR) \cong R/p^{i-1}R \neq 0$ for $i \geq 2$. Thus $pM \cong \bigoplus_{i\in I} R/p^{i-1}R \oplus \bigoplus_i C_i$ and $pN \cong \bigoplus_{i\in J} R/p^{i-1} \oplus R\bigoplus_i D_i$, and these expressions are direct sums of indecomposable modules. Since $pM \cong pN$, the uniqueness statement in the structure theorem for modules over a PID yields $I = J$ and after renumbering if necessary, $C_i \cong D_i$ for all i. The result follows.

4. Let G denote the Galois group of K over $\mathbb{Q}$. Then $|G| = 27$ and there is a one-to-one correspondence between subfields of K and subgroups of G which is reverse including. Also $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 9$ because f is irreducible with degree 9. Therefore $\mathbb{Q}(\alpha)$ corresponds to a subgroup H of order 3. To find a subfield of $\mathbb{Q}(\alpha)$ which has degree 3 over $\mathbb{Q}$, we need to find a subgroup of order 9 which contains H. Since G is a nontrivial finite 3-group, it contains a central subgroup Z of order 3. If Z is not contained in H, then $H \cap Z = 1$, hence

$$|HZ|/3 = |HZ|/|Z| = |HZ/Z| = |H/H \cap Z| = |H| = 3$$

and we see that HZ is a subgroup of order 9 containing H. On the other hand if $Z \subseteq H$, then $H = Z$ and hence $H \lhd G$. Thus G/H is a group of order 9, and hence has a subgroup of order 3, which by the subgroup correspondence theorem we may write as K/H, where K is a subgroup of G containing H. The order of K is $3|H| = 9$, which finishes the proof.

5. We note that given $a, b \in A$, there exists $n \in \mathbb{N}$ and $c \in A$ such that $p^n a = 0$ and $p^n c = b$. This shows that for $a, b \in A$,

$$a \otimes b = a \otimes p^n c = p^n a \otimes c = 0 \otimes c = 0.$$

Since $A \otimes A$ is generated as an abelian group by "simple tensors" $a \otimes b$, we deduce that every element of $A \otimes_{\mathbb{Z}} A$ is zero, in other words $A \otimes_{\mathbb{Z}} A = 0$.

6. The minimal polynomial divides the characteristic polynomial, so is x, x^2 or x^3. Also since the minimal polynomial factors into linear factors over k, the Jordan canonical form for A is defined over k.

   If the minimal polynomial is x, then $A = 0$, so we could take $B = 0$, since then $B^2 = 0 = A$.

If the minimal polynomial is x^2, then the invariant factors of A are x, x^2. Consider the matrix

$$C := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then $C \neq 0$ and $C^2 = 0$, so the invariant factors of C are x, x^2 and therefore C is similar to A. Thus it will be sufficient to find a matrix B such that $B^2 = C$; here we could take B to be

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

Then $B^2 = C$ as required.

Finally suppose A has one invariant factor, which will necessarily be x^3. Then the Jordan canonical form of A is

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

Suppose there is a matrix B such that $B^2 = A$. Then $B^6 = A^3 = 0$. Therefore the minimal polynomial of B divides x^6 and since B is a 3 by 3 matrix, we deduce that the minimal polynomial of B divides x^3. Therefore $B^3 = 0$ and we conclude that $A^2 = B^4 = 0$. But

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

which is nonzero, and the result follows.

7. Let K denote the field of fractions of R and let I denote the ideal of $K[x_1, \ldots, x_n]$ generated by S. Then $Z(S) = \{(r_1, \ldots, r_n) \in R^n \mid f(r_1, \ldots, r_n) = 0\}$ for all $f \in I$. By Hilbert's basis theorem, there is a finite subset T of S which generates the ideal I. Then $Z(S) = Z(T)$.

Algebra Prelim Solutions, January 2012

1. Let $n = |G|$. Then G has an element x of order n. However if H is any proper subgroup of G, then every element of H has order strictly less than n. Thus x cannot be in any proper subgroup of G and the result follows.

2. Suppose G be a simple group of order 6435. Then the number of Sylow 5-subgroups is congruent to 1 mod 5 and divides $9 \cdot 11 \cdot 13$. Furthermore this number is not 1 because G is not simple. Therefore this number must be 11 and it follows that G has a subgroup of index 11. Since G is simple, we deduce that G is isomorphic to a subgroup of S_{11} (even A_{11}). This is not possible because 13, and hence 6435, does not divide $11! = |S_{11}|$. We conclude that there is no simple group of order 6435 as required.

3. Define $\theta\colon \mathrm{M}_2(\mathbb{Q}) \times \mathrm{M}_2(\mathbb{Q}) \to \mathrm{M}_2(\mathbb{Q})$ by $\theta(A,B) = AB$. It is easily checked that θ is an $\mathrm{M}_2(\mathbb{Z})$-balanced map. Therefore θ induces a group homomorphism

$$\phi\colon \mathrm{M}_2(\mathbb{Q}) \otimes_{\mathrm{M}_2(\mathbb{Z})} \mathrm{M}_2(\mathbb{Q}) \to \mathrm{M}_2(\mathbb{Q}).$$

   It is easy to see that this map is a $(\mathrm{M}_2(\mathbb{Q}), \mathrm{M}_2(\mathbb{Q}))$-bimodule map. It remains to prove that ϕ is bijective, and we do this by producing the inverse map. Define $\psi\colon \mathrm{M}_2(\mathbb{Q}) \to \mathrm{M}_2(\mathbb{Q}) \otimes_{\mathrm{M}_2(\mathbb{Z})} \mathrm{M}_2(\mathbb{Q})$ by $\psi(A) = A \otimes 1$. It is clear that $\phi\psi$ is the identity, so it remains to prove that $\phi\psi$ is the identity. Since ϕ and ψ are both group homomorphisms, it will be sufficient to show that $\psi\phi$ is the identity on simple tensors, that is $\psi\phi(A \otimes B) = A \otimes B$. Therefore we need to prove that $AB \otimes 1 = A \otimes B$.

   Choose a positive integer n such that $Bn \in \mathrm{M}_2(\mathbb{Z})$. Then

$$AB \otimes 1 = \frac{A}{n}(Bn) \otimes 1 = \frac{A}{n} \otimes Bn = \frac{A}{n} n \otimes B = A \otimes B,$$

   and the result is proven.

4. By the structure theorem for finitely generated modules over a PID, M is a direct sum of modules of the form R and R/p^n where p is a prime in R and n is a positive integer. If M is nonzero, then it must contain a summand which is either isomorphic to R or R/p^nR, where p is a prime in R. Since M is injective and R is a domain, $rM = M$ for all $r \in R \setminus 0$, in particular $pM = M$ for primes p in R. Thus M cannot contain a summand isomorphic to R/p^nR. On the other hand if M contains a summand isomorphic to R, let

p be a prime in R, which exists because R is not a field. Since $pR \neq R$, we see that $pM \neq M$, a contradiction and the result follows.

5. (a) Obviously $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{2p})$, because $\zeta_{2p}^2 = \zeta_p$. On the other hand $\zeta_{2p} = -\zeta_p$, hence $\mathbb{Q}(\zeta_{2p}) \subseteq \mathbb{Q}(\zeta_p)$ and the result follows.

   (b) Set $f(x) = 1 + x^2 + \cdots + x^{2p-2}$. Since $f(x)(1-x^2) = 1 - x^{2p}$ and $\zeta_p, \zeta_{2p} \neq \pm 1$, we see that ζ_p and ζ_{2p} both satisfy $f(x)$. Thus the minimal polynomial of both these divides $f(x)$. Now ζ_p satisfies $g(x) := 1 + x + \cdots + x^{p-1}$. By making the substitution $y = x + 1$, we see that $g(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein for the prime p. Since $\deg(g) = p - 1 \geq 1$, it is also irreducible in $\mathbb{Q}[x]$. It follows that $g(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$. Also by considering the automorphism of $\mathbb{Q}[x]$ induced by $x \mapsto -x$, we see that $g(-x)$ is the minimal polynomial of ζ_{2p} over $\mathbb{Q}$, so $g(-x)$ divides $f(x)$. It follows that $f(x) = g(x)g(-x)$, the product of two irreducible polynomials.

6. Set $f(x) = x^5 - 5x - 1$. Then $f'(x) = 5x^4 - 5 = 5(x^2+1)(x-1)(x+1)$. Thus $f(x)$ has a maximum at -1, a minimum at 1. Since $f(1) > 0$ and $f(-1) < 0$, we find that f has exactly 3 real roots and 2 complex roots. We want to prove that f is irreducible (as a polynomial in $\mathbb{Q}[x]$). By Gauss's lemma, if f is not irreducible, then we may write $f = gh$ where $g, h \in \mathbb{Z}[x]$, $\deg g, \deg h \geq 1$, and g, h are monic. Neither of g, h has degree one, because ± 1 is not a root of f. Therefore we may without loss of generality assume that $\deg g = 3$ and $\deg h = 2$, say $g = x^3 + ax^2 + bx + c$ and $h = dx + e$, where $a, b, c, d, e \in \mathbb{Z}$. By equating coefficients, we find that $a + d = 0$, $ad + bc + e = 0$, $ae + bd + c = 0$, $be + cd = 1$, $ce = 1$. Thus $c, e = 1$ or $c, e = -1$, and we find that $a^2 \pm a + 1 = 0$. This last equation has no root in $\mathbb{Z}$ and we conclude that f is irreducible.

   Let G denote the Galois group of f over $\mathbb{Q}$. We consider G as a subgroup of S_5 (by permuting the 5 roots of f). Since f is irreducible and 5 is prime, we see that G contains a 5-cycle. Also G contains a transposition, namely complex conjugation. Since S_5 is generated by a 5-cycle and a transposition, we deduce that $G \cong S_5$.

7. (a) We may write the general element of $\mathbb{Q}[x, y]$ as $f_0 + f_1 y + f_2 y^2 + \cdots + f_n y^n$, where n is a positive integer and $f_i \in \mathbb{Q}[x]$ for all i. Then modulo the ideal $(x^3 - y^2)$, we may replace y^2 with x^3 everywhere and we see

that every element of $\mathbb{Q}[x,y]$ can be written in the form $f+gy+(x^3-y^2)h$, where $f,g\in\mathbb{Q}[x]$ and $h\in\mathbb{Q}[x,y]$. The result follows.

(b) Define a ring homomorphism $\theta\colon \mathbb{Q}[x,y]\to\mathbb{Q}[t]$ by $\theta(x)=t^2$, $\theta(y)=t^3$ and $\theta(q)=q$ for $q\in\mathbb{Q}$. Then $\operatorname{im}\theta=\mathbb{Q}[t^2,t^3]$. Also if $h\in\ker\theta$, write $h=k+f+yg$, where $k\in(x^3-y^2)$, and $f,g\in\mathbb{Q}[x]$. Then $\theta(h)=f(t^2)+t^3g(t^2)$. Since $f(t^2)$ is a polynomial involving only even powers of t and $t^3g(t^2)$ is a polynomial involving only odd powers of t, we see that $\theta(h)$ can only be zero if $f,g=0$. It follows that $\ker\theta=(x^3-y^2)$ and the result now follows from the fundamental homomorphism theorem. Note that we have also proven that if $h(x^2,x^3)=0$, then $h\in(x^3-y^2)$.

(c) Note that t^2 and t^3 are irreducible in $\mathbb{Q}[t^2,t^3]$ (use unique factorization in $\mathbb{Q}[t]$). Since $t^6=(t^2)^3=(t^3)^2$, two different ways of factoring t^6, we see that $\mathbb{Q}[t^2,t^3]$ is not a UFD.

(d) Note that $\mathscr{Z}(x^3-y^2)=\{(t^2,t^3)\mid t\in\mathbb{Q}\}$. Indeed $(t^2,t^3)\in\mathscr{Z}(x^3,y^2)$, because $(t^2)^3-(t^3)^2=0$. On the other hand if $(p,q)\in\mathscr{Z}(x^3-y^2)$, write $t=q/p$ ($t=0$ if $p=0$). Since $p^3=q^2$, we see that $p=t^2$ and $q=t^3$. Now suppose f is a polynomial vanishing on V. Then $f(t^2,t^3)=0$ for all $t\in\mathbb{Q}$. Since $\mathbb{Q}$ is infinite, we see that $f(x^2,x^3)=0$ and it follows from (b) that $f\in(x^3-y^2)$. It follows that the coordinate ring $\mathbb{Q}[V]$ of V is $\mathbb{Q}[x,y]/(x^3-y^2)\cong\mathbb{Q}[x^2,x^3]$ by (b).

(e) Since $\mathbb{Q}$ is an infinite field, $\mathbb{A}^1$ has coordinate ring $\mathbb{Q}[x]$, a UFD. But $\mathbb{Q}[V]$ is not a UFD by (c), in particular $\mathbb{Q}[\mathbb{A}^1]$ is not isomorphic to $\mathbb{Q}[V]$. Since isomorphic affine algebraic sets have isomorphic coordinate rings, we deduce that V is not isomorphic to $\mathbb{A}^1$.

Algebra Prelim Solutions, August 2013

1. We use without further comment the property that a p-subgroup of a group is a Sylow p-subgroup if and only if it has index in the group prime to p.

   First suppose P is a Sylow p-subgroup of G. Then $P \cap H$ is a subgroup of P, so $P \cap H$ is a p-subgroup of H. Also $P/P \cap H \cong PH/H$, hence $|H|/|P \cap H| = |PH|/|P|$. Furthermore $|G|/|P| = |G|/|PH| \cdot |PH|/|P|$ and we deduce that $|H|/|P \cap H|$ divides $|G|/|P|$. Since $|G|/|P|$ is prime to p, it follows that $|H|/|P \cap H|$ is also prime to p, which proves that $P \cap H$ is a Sylow p-subgroup of H.

   Next, $PH/H \cong P/P \cap H$, so PH/H is a p-subgroup of G/H. Furthermore $|G|/|P| = |G|/|PH| \cdot |PH|/|P|$, and we see that $|G|/|PH|$ is prime to p. Therefore $|G/H|/|PH/H|$ is also prime to p and it follows that PH/H is a Sylow p-subgroup of G/H.

   Now suppose $P \cap H$ and PH/H are Sylow p-subgroups. Since $P/P \cap H \cong PH/H$ and $|P| = |P/P \cap H| \cdot |P \cap H|$, we see that P is a p-group. Finally if $|H| = p^a x$ and $|G/H| = p^b y$, where x and y are prime to p, then $|G| = p^{a+b}xy$ and xy is prime to p. This means that a Sylow p-subgroup of G has order p^{a+b}. But since $|P \cap H| = p^a$ and $|PH/H| = p^b$, we see that $|P| = p^{a+b}$ and hence P is a Sylow p-subgroup of G, as required.

2. Suppose G is simple group of order 576. The number of Sylow 2-subgroups is congruent to 1 mod 2 and divides 9, so has to be 1, 3 or 9. It cannot be 1, because then G would have a normal Sylow 2-subgroup. Nor can it be 3, otherwise G would be isomorphic to a subgroup of A_3. Finally suppose it is 9. Then G is isomorphic to a subgroup of A_9; unfortunately at first sight this seems possible, because 576 divides $|A_9|$. However the isomorphism is induced by the representation of G on the 9 left cosets of a Sylow 2-subgroup P in G. Thus $g \in G$ gives the permutation $xP \mapsto gxP$. Then g stabilizes some xP if and only if g is in some Sylow 2-subgroup. So if g has order 6, it can be considered as an element of A_9 which fixes no points; a quick check shows that this is not possible and therefore G has no element of order 6.

   Now consider the Sylow 3-subgroups. If P and Q are distinct Sylow 3-subgroups and $1 \neq x \in P \cap Q$, then $\mathrm{C}_G(x)$ contains P and Q and hence contains an element of order 2. It follows that G has an element of order 6, which is not possible by the previous paragraph, so distinct Sylow 3-subgroups intersect trivially.

Next the number of Sylow 3-subgroups is 16 or 64. If it is 16, we consider the representation of G on the left cosets of a Sylow 3-subgroup P. If Q is another Sylow 3-subgroup, then there is an orbit under Q which has order 3, which shows that there exists $1 \neq q \in Q$ such that $q \in P \cap Q$, contradicting the previous paragraph. Finally if there are 64 Sylow 3-subgroups, then since two distinct Sylow 3-subgroups intersect in the identity, we can count elements to show that G has a normal Sylow 2-subgroup.

3. Consider $p^m + q^n$. If this is not a unit, then there exists some prime which divides it, which without loss of generality we may assume is p. Thus p divides $p^m + q^n$, hence p divides q^n, which is not possible.

   Now let $I \lhd R$. We want to prove I is a principal ideal, and since 0 is clearly a principal ideal, we may assume that $I \neq 0$. Each nonzero element of I has a factorization up^iq^j, where u is a unit and i, j are nonnegative integers. Choose $0 \neq x \in I$ such that $x = p^iq^j$, with i as small as possible, and then choose $0 \neq y \in I$ such that $y = p^kq^l$, with l as small as possible. We will show that $I = (p^iq^l)$. Clearly $I \subseteq (p^iq^l)$. On the other hand $p^{k-i} + q^{j-l}$ is a unit by the above, hence p^iq^l is an associate of $y+x$ and we see that $p^iq^l \in I$. This proves that $I = (p^iq^l)$.

4. Note that $k[x]$ is a PID. By the structure theorem for finitely generated modules over a PID, we may write $M \cong k[x]^d \oplus k[x]/(f_1) \oplus \cdots \oplus k[x]/(f_n)$, where the f_i are monic polynomials, say of degree a_i, and $f_i \mid f_{i+1}$ for all i. Suppose $d = 0$. Then $\dim_k M = \sum_{i=1}^n a_i$, and then it is clear that if N is a proper $k[x]$-submodule of M, then $N \ncong M$, because $\dim_k N < \dim_k M$. Therefore $d > 0$, in particular there is an epimorphism $M \twoheadrightarrow k[x]$. Since C is a cyclic $k[x]$-module, there exists an epimorphism $k[x] \twoheadrightarrow C$. By composing these two epimorphisms, we obtain a $k[x]$-module epimorphism $M \twoheadrightarrow C$.

5. Let p denote the characteristic of K. Then we may write $|K| = p^n$ where $n \in \mathbb{N}$. Set $M = K^+ \otimes_{\mathbb{Z}} L^\times$. Then $|K^+|M = 0$ and $|L^\times|M = 0$, so if $(|K|, |L| - 1) = 1$, we see that $|M| = 0$. Now suppose $(|K|, |L| - 1) \neq 1$. Then p divides $|L| - 1$. Also $K^+ \cong (\mathbb{Z}/p\mathbb{Z})^n$ and $L^\times \cong \mathbb{Z}/(|L| - 1)\mathbb{Z}$.

   Now we have well defined homomorphisms $\theta : \mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(|L| - 1)\mathbb{Z}$ and $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(|L| - 1)\mathbb{Z}$ determined by $\theta(\bar{x} \otimes \bar{y}) = \overline{xy}$ and $\phi(\bar{x}) = \bar{x} \otimes \bar{1}$, and $\theta\phi$ and $\phi\theta$ are the identity maps. This shows that $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(|L| - 1)\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$ and we deduce that $M \cong (\mathbb{Z}/p\mathbb{Z})^n$. Therefore if $(|K|, |L| - 1) \neq 1$, it follows that $|M| = |K|$.

6. Write $K \cap L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, let f_i denote the minimum polynomial of α_i over $\mathbb{Q}$, and set $f = f_1 \ldots f_n$. Let F denote the splitting field of f over $\mathbb{Q}$, a subfield of $\mathbb{C}$. Since K and L are Galois extensions of $\mathbb{Q}$, all the roots of all f_i lie in both K and L and hence the splitting field of f is contained in $K \cap L$. Therefore $K \cap L$ is the splitting field of f and it follows that $K \cap L$ is a Galois extension of $\mathbb{Q}$.

7. We can split up the given exact sequence into two short exact sequences, namely $0 \to \mathbb{Z} \to P \to Y \to 0$ and $0 \to Y \to Q \to \mathbb{Z} \to 0$. Then using the long exact sequence for Ext in the first variable, we obtain

$$H^1(G,X) = \mathrm{Ext}^1_{\mathbb{Z}G}(\mathbb{Z},X) \cong \mathrm{Ext}^2_{\mathbb{Z}G}(Y,X) \cong \mathrm{Ext}^3_{\mathbb{Z}G}(\mathbb{Z},X) = H^3(G,X),$$

as required.

Algebra Prelim Solutions, August 2014

1. (a) If $x \in X$, then $o(g)$ is a power of p, and since $o(g) = o(xgx^{-1})$, we see that $o(g \cdot x) \in X$. Also $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = (gh) \cdot x$ for $g, h \in P$. Finally $1 \cdot x = x$, and so we have an action.

   (b) $\{z\}$ is an orbit of size 1 if and only if $g \cdot z = z$ for all $g \in P$, if and only if z is in the center of P.

   (c) The size of the orbits divide $|P|$ and therefore are powers of p. Let Z denote the center of G. By (b), the number of orbits of size 1 is $|Z|$. Since $p \mid |G|$, we see that $p \mid |P|$ and hence $p \mid |Z|$, because the center of a nontrivial p-group is nontrivial. The result follows.

2. We prove the result by induction on $|G|$. We may assume that $G \neq 1$, because if G is the trivial group, then G has no maximal subgroups. Let Z denote the center of G and first suppose $H \supseteq Z$. By subgroup correspondence theorem, H/Z is a maximal subgroup of G/Z. By induction, $H/Z \lhd G/Z$ and $|\frac{G/Z}{H/Z}| = p$. Therefore $H \lhd G$ and $|G/H| = p$.

   Now assume that $H \not\supseteq Z$. Since $HZ \leq G$ and $HZ \neq H$, we see that $HZ = G$. Since the normalizer of H in G contains H and Z, we see that $H \lhd G$. Since G/H is a nontrivial p-group, its center Y/H is nontrivial and we see that $Y = G$, by maximality of H. Therefore G/H is abelian. But then G/H has a subgroup K/H of order p, and we must have $K = G$, again by maximality of H, and the result is proven.

3. Let $I \lhd R$. Since R is noetherian, there exist $x_1, \ldots, x_n \in R$ such that $I = (x_1, \ldots, x_n)$. Let g denote the greatest common divisor of $\{x_1, \ldots, x_n\}$. Since $g \mid x_i$ for all i, there exist $r_i \in R$ such that $x_i = gr_i$ and we see that $I \subseteq (g)$. Also $x_i/g \in R$ for all i and no prime divides all the x_i. Therefore $(x_1/g, \ldots, x_n/g) = R$, in particular there exist $s_i \in R$ such that $x_1s_1/g + \cdots + x_ns_n/g = 1$ and hence $g = x_1s_1 + \ldots x_ns_n$. Therefore $g \in I$, consequently $I = (g)$ and it follows that R is a PID, as required.

4. Since M is an injective $\mathbb{Z}$-module over the PID I and $q \neq 0$, we see that $qM = M$. Now let $m \otimes z$ be a simple tensor in $M \otimes_{\mathbb{Z}} \mathbb{Z}$. Since $qM = M$, there exists $n \in M$ such that $qn = m$ and the

$$m \otimes z = qn \otimes z = n \otimes qz = n \otimes 0 = 0.$$

Since every tensor is a sum of simple tensors, it follows that $M \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z} = 0$.

5. Since M is a finitely generated module over the PID $\mathbb{C}[x]$, we may write $M = F \oplus T$, where F is a free $\mathbb{C}[x]$-module of finite rank and T is a finitely generated torsion module. Furthermore we may write $F = \bigoplus_{i=1}^{n} \mathbb{C}[x]/(x-a_i)^{b_i}$ for some integers n, b_i and $a_i \in \mathbb{C}$. First suppose $F = 0$. Note that $\dim_{\mathbb{C}} T < \infty$, so $\dim_{\mathbb{C}} M < \infty$, in particular no such N can exist ($\dim_{\mathbb{C}} M = \dim_{\mathbb{C}} N \Rightarrow M \cong N$ as $\mathbb{C}$-modules).

   Therefore we may assume that $F \neq 0$. Now choose any $c \in \mathbb{C}$ with $c \neq a_i$ for all i. By the Chinese remainder theorem $(x-c)T = T$. Also $(x-c)F \cong F$ and hence $(x-c)M \cong M$. Finally $F = \mathbb{C}[x]^m$ for some $m \in \mathbb{N}$, consequently $(x-c)F = (x-c)\mathbb{C}[x]^m$ and we deduce that $(x-c)F \neq F$. Therefore $(x-c)M \neq M$ and the result follows (in fact there exist infinitely many such c).

6. (a) A polynomial has a degree 1 factor if and only if it has a root. Therefore a degree 2 polynomial $f \in \mathbb{F}_2[x]$ is irreducible if and only if $f(0) = f(1) = 1$. There are only 4 degree 2 polynomials, and it is easy to see that only $x^2 + x + 1$ satisfies this criterion.

   (b) If $g := x^5 + x^3 + 1$ is not irreducible, it has a factor of degree 1 or 2. But $g(0) = g(1) = 1$ and $x^2 + x + 1$ does not divide g. Therefore g is irreducible and it follows that $[\mathbb{F}_2(\alpha) : \mathbb{F}] = 5$. If $h := x^4 + x + 1$ is not irreducible, it has a factor of degree 1 or 2. But $h(0) = h(1) = 1$ and $x^2 + x + 1$ does not divide h. Therefore h is also irreducible and it follows that $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 4$. Since 4 and 5 are coprime, we deduce that $[\mathbb{F}_2(\alpha, \beta) : \mathbb{F}_2] = 4 \cdot 5 = 20$.

   (c) Since all field extensions involving finite fields are Galois extensions, $K = \mathbb{F}_2(\alpha, \beta)$. Also we know that the Galois group is cyclic with order the degree of the extension. Therefore $\mathrm{Gal}(K/\mathbb{F}_2) \cong \mathbb{Z}/20\mathbb{Z}$.

7. First we compute the character table for S_3. There are three conjugacy classes in S_3, and representatives are 1, $(1\ 2)$ and $(1\ 2\ 3)$. There is the trivial representation with character χ_1 defined by $\chi_1(x) = 1$ for all $x \in S_3$. Then there is the character χ_2 which is defined by the sign of a permutation, so $\chi_2(1) = \chi_2(1\ 2\ 3) = 1$ and $\chi_2(1\ 2) = -1$. The number of irreducible characters equals the number of conjugacy classes, so there are exactly three irreducible characters. The final character χ_3 can be determined by the orthogonality relations. We have $\chi_3(1) = 2$. Since χ an irreducible character

if and only if $\overline{\chi}$ (complex conjugate) is an irreducible character, we see that $\chi_3(1\ 2)$ and $\chi_3(1\ 2\ 3)$ are real numbers. Taking the inner product of the first two columns of the character table, we obtain $\chi_3(1\ 2) = 0$, and then it follows easily that $\chi_3(1\ 2\ 3) = -1$. Thus the character table of S_3 is

Class Size	1	3	2
Class Rep	1	$(1\ 2)$	$(1\ 2\ 3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	1	0	-1

Since $\mathbb{Z}/3\mathbb{Z}$ is an abelian group, all its irreducible characters are of degree one and correspond to homomorphisms into the cube roots of 1 in $\mathbb{C}$, because $|\mathbb{Z}/3\mathbb{Z}| = 3$. Let $\omega = e^{2\pi i/3}$, a primitive cube root of 1. Let 0, 1, 2 represent the conjugacy classes $\bar{0}$, $\bar{1}$, $\bar{2}$ respectively. Then the character table for $\mathbb{Z}/3\mathbb{Z}$ is

Class Size	1	1	1
Class Rep	0	1	2
ψ_1	1	1	1
ψ_2	1	ω	ω^2
ψ_3	1	ω^2	ω

Now for a finite group of the form $G \times H$, the conjugacy classes of $G \times H$ is $C \times D$, where C is the set of conjugacy classes of G and D is the set of conjugacy classes of D, and then the irreducible characters are of the form $\chi_i \psi_j := \chi_i(c)\psi_j(d)$, in particular there are $|C| \cdot |D|$ irreducible characters. Therefore the character table of $S_3 \times \mathbb{Z}/3\mathbb{Z}$ is

Class Size	1	1	1	3	3	3	2	2	2
Class Rep	(1,0)	(1,1)	(1,2)	((1 2),0)	((1 2),1)	((1 2),2)	((1 2 3),0)	((1 2 3),1)	((1 2 3),2)
$\chi_1\psi_1$	1	1	1	1	1	1	1	1	1
$\chi_1\psi_2$	1	ω	ω^2	1	ω	ω^2	1	ω	ω^2
$\chi_1\psi_3$	1	ω^2	ω	1	ω^2	ω	1	ω^2	ω
$\chi_2\psi_1$	1	1	1	-1	-1	-1	1	1	1
$\chi_2\psi_2$	1	ω	ω^2	-1	$-\omega$	$-\omega^2$	1	ω	ω^2
$\chi_2\psi_3$	1	ω^2	ω	-1	$-\omega^2$	$-\omega$	1	ω^2	ω
$\chi_3\psi_1$	2	2	2	0	0	0	-1	-1	-1
$\chi_3\psi_2$	2	2ω	$2\omega^2$	0	0	0	-1	$-\omega$	$-\omega^2$
$\chi_3\psi_3$	2	$2\omega^2$	2ω	0	0	0	-1	$-\omega^2$	$-\omega$

Algebra Prelim Solutions, August 2015

1. (a) Let U denote the upper unitriangular matrices of G and let D denote the diagonal matrices of G. Then it is easily checked that $U \lhd G$, $|U| = 5^3$, and that $|D| = 4^3$. Therefore G has a normal Sylow 5-subgroup, which means it is unique and so $P_5 = U$.

   (b) Let

$$Z = \{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid z \in \mathbb{F}_5 \} \text{ and let } N = \{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a,b \in \mathbb{F}_5 \}.$$

   Then $N, Z \lhd G$ (in fact Z is the center of G) and $1 \lhd Z \lhd N \lhd G$ is a composition series (in fact a chief series) for G, with corresponding quotients isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

   (c) Set $P_2 = D$ (note that P_2 is a Sylow 2-subgroup of G, however it is not normal and thus there are other choices for a Sylow 2-subgroup of G). Then $P_2 \cap P_5 = 1$, and since $|P_2| \cdot |P_5| = |G|$, it follows that G is isomorphic to the semidirect product $P_2 \ltimes P_5$.

2. (a) Let $0 \neq u \in U$. Then $u_d \neq 0$ (dth entry of u) for some d, where $1 \leq d \leq n$. Let E_{ij} denote the matrix unit that has 1 in the (i,j)th position and zeros elsewhere. Then $E_{id}u = u_d v_i$, where v_i is the column vector that has 1 in the ith position and zeros elsewhere. It follows easily that U contains $\mathbb{F}^n$ and hence U is simple as required.

   (b) Note that S is a direct sum of n copies of V as an S-module. Thus V is a projective S-module, because it is a direct summand of S. Also if I is a left ideal of S, then it has a composition series as an S-module such that each composition factor is isomorphic to V. Since V is projective, it follows that S is a direct sum (of a finite number) of copies of S and the result follows.

3. Let $\omega = \frac{-1 \pm i\sqrt{3}}{2}$, a primitive cube root of 1. Then the roots of $x^{12} - 1$ are $i^a \omega^b$, where $0 \leq a \leq 3$ and $0 \leq b \leq 2$. Also the roots of $x^2 - 2x + 2$ are $1 \pm i$. It follows easily that a splitting field K for $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt{2})$. Now $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$ are Galois extensions of $\mathbb{Q}$ of degree 2. Thus $[K : \mathbb{Q}] \leq 4$. Also $i \notin \sqrt{3}$ and it follows that $[K : \mathbb{Q}] = 4$. We conclude that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\alpha, \beta \in \mathrm{Gal}(K/\mathbb{Q})$ be defined by $\alpha i = -i$, $\alpha\sqrt{3} = \sqrt{3}$, $\beta i = i$, $\beta\sqrt{3} = -\sqrt{3}$. Then α, β have order 2 and $\mathrm{Gal}(K/\mathbb{Q}) = \langle \alpha \rangle \times \langle \beta \rangle$.

4. Let A be a 5×5 matrix of order 3. Then its minimal polynomial divides $x^3 - 1$ and is not $x - 1$.

   (a) We use the rational canonical form to determine the conjugacy classes in $\mathrm{GL}_5(\mathbb{Q})$ (assume this is what the question means). Here the minimal polynomial must be $(x-1)(x^2+x+1)$ and there are two possibilities for the invariant factors, namely $\{x-1, x-1, x^3-1\}$ and $\{x^2+x+1, x^3-1\}$. It follows that there are two conjugacy classes of matrices of order 3. The corresponding matrices are

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

   (b) We use the Jordan canonical form to determine the conjugacy classes in $\mathrm{GL}_5(\mathbb{C})$ (again, assume this is what the question means). Since A has finite order, its Jordan canonical form will be a diagonal matrix and hence the conjugacy classes will be determined by the eigenvalues of A (including multiplicities). Let $\omega = e^{2\pi i/3}$, a primitive cube root of 1. Now the eigenvalues are the cube roots of 1, there must be 5 eigenvalues, and not all the eigenvalues can be 1 because A is not the identity. It follows that a set of representatives for the conjugacy classes over $\mathbb{Q}$ are $\{\mathrm{diag}(1, \ldots, \omega, \ldots, \omega^2)\}$, where there is at most four 1's, and otherwise arbitrary.

   If one wants to find out precisely how many conjugacy classes, note that the number without the restriction that there are at most four ones is the coefficient of x^5 in

$$(1 + x + x^2 + \cdots)^3 = (1-x)^{-3},$$

   that is $7!/(2! \cdot 5!) = 21$. Therefore the number of conjugacy classes is 20.

5. (a) Clearly if $M = 0$, the $M_P = 0$ for all prime ideals P. Conversely suppose $M_P = 0$ for all prime ideals P and let $0 \neq m \in M$; we need to show that no such m exists. Define $I = \{r \in R \mid rm = 0\}$. Then I is a proper ideal of R and therefore it is contained in a maximal ideal P. Since maximal

ideals are prime, P is a prime ideal. Now $M_P = 0$ tells us that $sm = 0$ for some $s \in R \setminus P$, and we now have a contradiction as required.

(b) It is obvious that if $f\colon M \to N$ is surjective then $f_P\colon M_P \to N_P$ is surjective, so we need to prove the converse. Now localization is an exact functor, in particular $M_P \to N_P \to (M/N)_P \to 0$ is exact. Therefore if f_P is surjective for all prime ideals P, we see that $(M/N)_P = 0$ for all prime ideals P, and then we deduce from (a) that $M/N = 0$. This completes the proof.

6. Note that a Sylow p-subgroup has order p, in particular a Sylow p-subgroup is a nontrivial proper subgroup of G. We'll consider the cases $a = 1, 2, 3$ separately. First suppose $a = 1$. Then the number of Sylow p-groups is congruent to 1 mod p and divides 2 and we see that there is exactly one Sylow p-subgroup. Thus the Sylow p-subgroup is normal and we see that G is not simple.

   Next suppose that $a = 2$. Then the number of Sylow p-groups is congruent to 1 mod p and divides 4 and we see that there is exactly one Sylow p-subgroup unless $p = 3$ and we conclude that G is not simple. On the other hand if $p = 3$ and G is simple, then G is isomorphic to a subgroup of A_3 because G has a subgroup of index 3, namely a Sylow 2-subgroup. This is clearly not possible because $|G| = 12$ and $|A_3| = 3$. We deduce that in all cases, G is not simple.

   Finally suppose that $a = 3$. Then the number of Sylow p-groups is congruent to 1 mod p and divides 8 and we see that there is exactly one Sylow p-subgroup unless $p = 3$ or 7. If $p = 3$, then the Sylow 2-subgroup has index 3 in G, so if G is simple, we see that G is isomorphic to a subgroup of A_3. This is not possible because $|G| = 24$ and $|A_3| = 3$. Now suppose that $p = 7$. Then the number of Sylow 7-subgroups is congruent to 1 mod 7 and divides 8. If there is 1, then the Sylow 7-subgroup is normal, so if G is simple, then there are 8 Sylow 7-subgroups. Since two distinct subgroups of order 7 intersect in the identity, we see that there are 48 elements of order 7 in G. Also if the Sylow 2-subgroup is not normal, there are at least 9 elements of order a power of 2, so G has at least $48 + 9 = 57$ elements, which is not possible. We conclude that in all cases, G is not simple.

7. It is obvious that each statement implies the next, because at each stage given a solution, we use the images of that solution for the next stage.

(c) implies (b). Write $n = p_1^{e_1} p_2^{e_2} \dots p_d^{e_d}$, where the p_i are distinct primes, and $d, e_i \in \mathbb{N}$. Suppose we have solutions $(a_{1,i}, \dots a_{m,i})$ in $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ for all i. By the Chinese remainder theorem, we may choose $a_1, \dots, a_m \in \mathbb{Z}/n\mathbb{Z}$ such that $a_i \equiv a_{ij} \mod \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ for all i. Then $(a_1, \dots, a_m)$ is a solution in $\mathbb{Z}/n\mathbb{Z}$.

(c) doesn't imply (a). Consider the polynomial $f(x) = (x^2+x+1)(x^3-7)(x^5-2)$. Clearly f has no root in $\mathbb{Z}$. We need to show that f has a root in $\mathbb{Z}/p^n\mathbb{Z}$, for all primes p and $n \in \mathbb{N}$. Recall that the multiplicative group $U(p^n)$ of nonzero elements of $\mathbb{Z}/p^n\mathbb{Z}$ has order $p^{n-1}(p-1)$. If $3 \mid p-1$, then $U(p^n)$ has an element α of order 3. If $\alpha \equiv 1 \mod p$, then $\alpha^{p^n} = 1$ which is not the case. It follows that $\alpha - 1$ is a unit $\mathbb{Z}/p^n\mathbb{Z}$ and since $(\alpha - 1)(\alpha^2+\alpha+1) = 0$, we deduce that α is a root of x^2+x+1 and hence also a root of f. On the other hand if $3 \mid p-2$, then $(3, |U(p^n)|) = 1$ and $7 \in U(p^n)$, and therefore there exists $\beta \in U(p^n)$ such that $\beta^3 = 7$. It again follows that f has root in $\mathbb{Z}/p^n\mathbb{Z}$. If $p = 3$, then $2 \in U(3^n)$ and $(|U(3^n), 5) = 1$ and therefore there exists $\gamma \in U(3^n)$ such that $\gamma^5 = 2$. We have now shown that $f(x)$ has a root in $\mathbb{Z}/p^n\mathbb{Z}$ for all primes p and all $n \in \mathbb{N}$.

(d) doesn't imply (c). Consider the polynomial $f(x) = (x^2+x+1)(x^3-2)$. We first show that f has a root in $\mathbb{Z}/p\mathbb{Z}$ for all primes p. If $3 \mid p-1$, then $U(p)$ has an element of order 3 and we see that x^2+x+1 and hence also $f(x)$ has a root. On the other hand if $3 \mid p-2$ and $p \neq 2$, then $(|U(p)|, 3) = 1$ and since $2 \in U(p)$, we find that $x^3 - 2$ and hence also $f(x)$ has a root. Finally $f(0) = 0$ in $\mathbb{Z}/2\mathbb{Z}$ and $f(1) = 0$ in $\mathbb{Z}/3\mathbb{Z}$, and we have now shown that f has a root in $\mathbb{Z}/p\mathbb{Z}$ for all primes p. However $f(x) \neq 0$ for all $x \in \mathbb{Z}/4\mathbb{Z}$ (just plug in $x = 0, 1, 2, 3$).

Algebra Prelim Solutions, August 2016

1. (a) The number of Sylow 5-subgroups is congruent to 1 mod 5 and divides 48, so the possibilities are 1, 6 and 16. However G is simple, so 1 is not possible, nor is 6 because then G would be isomorphic to a subgroup of A_6 which has order 360, but $|G|$ does not divide 360. Therefore G has exactly 16 Sylow 5-subgroups, which means that G has a subgroup of order $240/16 = 15$. Let H be a group of order 15. The number of Sylow 3-subgroups is congruent to 1 mod 3 and divides 5, so there is a unique Sylow 3-subgroup A which must be normal. Similarly the number of Sylow 5-subgroups is congruent to 1 mod 5 and divides 3, so there is a unique Sylow 5-subgroup B which must be normal. Since $A \cap B = 1$ and $AB = H$, it follows that $H \cong A \times B$, so H is an abelian group of order 15 and it follows from the structure theorem for finitely generated abelian groups that H is cyclic.

   (b) From (a), we see that the normalizer of a Sylow 3-subgroup has a subgroup of order 15, and we deduce that the number of Sylow 3-subgroups divides $240/15 = 16$. Therefore number of Sylow 3-subgroups is congruent to 1 mod 3 and divides 16, so the possibilities are 1, 4 and 16. However 1 and 4 are not possible because G is simple. Therefore G has exactly 16 Sylow 3-subgroups. Since two distinct Sylow 3-subgroups intersect in the identity, we conclude that G has exactly 32 elements of order 3.

2. (a) Since each I_i is principal, there exist $a_i \in I_i$ such that $I_i = (a_i)$ for all $i \in \mathbb{N}$. Write $a_1 = up_1 \dots p_d$ where u is a unit and the p_i are primes. Since $(a_i) \subseteq (a_{i+1})$, we see that a_{i+1} divides a_i for all i. But R is a UFD, so either a_i and a_{i+1} are associates in which case $(a_i) = (a_{i+1})$, or a_{i+1} is divisible by at least one fewer prime of the primes in $\{p_1, \dots, p_d\}$ than a_i. The result follows.

   (b) Note that if I is an ideal generated by finitely many elements $a_1, \dots, a_d$ where $d \geq 2$, then (a_{d-1}, a_d) is principal, so is equal to (b) for some $b \in R$ and then $I = (a_1, \dots, a_{d-2}, b)$. Thus I can be generated by $d-1$ elements and it follows by induction on d that I is principal. Now let I be an arbitrary ideal. If I is not finitely generated, then we can find an infinite sequence $a_1, a_2, \dots \in I$ such that $a_{n+1} \notin (a_n)$. Set $I_n = (a_1, \dots, a_n)$. Then I_n is a principal ideal for all n because it is finitely generated. This contradicts (a).

3. (a) This is true. Since P is projective, we may write $P \oplus Q = F$, where F is a free S-module. Then

$$(R \otimes_S P) \oplus (R \otimes_S Q) \cong R \otimes_S (P \oplus Q) \cong R \otimes_S F.$$

Now $R \otimes_S S \cong R$ as left R-modules (via the map induced by $r \otimes s \mapsto rs$, which has inverse $r \mapsto r \otimes 1$). If F is free on X, then $R \otimes_S F$ is free on $1 \otimes x$, so $R \otimes_S P$ is a direct summand of the free R-module $R \otimes_S F$. This proves that $R \otimes_S P$ is a projective R-module.

(b) Let F be a field (e.g. $\mathbb{Q}$), let $S = F$ and let $R = F[x]$. Then S is an injective S-module (over a field all modules are both injective and projective; this is just a consequence of the fact that every subspace has a direct complement). On the other hand $R \otimes_S S \cong R$ (see above). This is not injective; consider the $F[x]$-submodule $xF[x]$ of $F[x]$. The map $f \mapsto xf$ show that $F[x] \cong xF[x]$, so if $xF[x]$ was injective, then $xF[x]$ would be also and we would conclude that $xF[x]$ is a direct summand of $F[x]$, say $F[x] = xF[x] \oplus K$, where K is an ideal of $F[x]$. Since $xF[x] \neq F[x]$ (because $xF[x]$ consists of polynomials of degree at least 1), we see that $K \neq 0$. Let $0 \neq k \in K$. Then $0 \neq xk \in xF[x] \cap K$, which contradicts the direct sum property. Therefore $F[x]$ is not an injective $F[x]$-module, as required.

4. We use the structure theorem for finitely generated modules over a PID, elementary divisor form. We may write

$$M \cong R^d \oplus \bigoplus_i (R/Rq_i)^{d_i}$$
$$N \cong R^e \oplus \bigoplus_i (R/Rq_i)^{e_i}$$

where $d, e, d_i, e_i \geq 0$, the q_i are distinct prime powers in R, and uniquely so apart from the possibility that some of the $d, e, d_i, e_i = 0$. Since $M^3 \cong N^2$, we deduce from uniqueness that $3d = 2e$ and $3d_i = 2e_i$ for all i. Therefore d and all d_i are divisible by 2 and we may set $P = R^{d/2} \bigoplus_i (R/Rq_i)^{d_i}$.

5. (a) Since A is similar to A^2, there exists an invertible matrix X such that $XAX^{-1} = A^2$ and we see that $XA^mX^{-1} = A^{2m}$ for all $m \in \mathbb{N}$. Then for $n \in \mathbb{N}$, we have

$$X^n A x^{-n} = X^{n-1} A^2 X^{-n+1} = X^{n-2} A^4 X^{2-n} = \cdots = A^{2n},$$

which proves that A is similar to A^{2n}.

(b) We show that the Jordan canonical form J for A is a diagonal matrix, which will prove the result because J is similar to A. Since A is similar to A^2, we see that J is similar to J^2 and by part (a), we deduce that J is similar to J^{2^n} for all $n \in \mathbb{N}$. Choose n greater than the size of the matrix A and set $e = 2^n$. We show that J^e is a diagonal matrix. Let $K = J(d,a)$ be a Jordan block of A, that is a $d \times d$ matrix with a's on the main diagonal and 1's on the superdiagonal. Then we may write $K = aI + N$ where I is the identity matrix. Note that aI and N commute, because everything commutes with the identity matrix, and $N^{d-1} = 0$, in particular $N^e = 0$. By Freshman's dream, we get $K^2 = a^2 I + N^2$, and repeating this n times, we obtain $K^e = a^e I$, a diagonal matrix, and the result follows.

6. Let $\omega = e^{2\pi i/7}$, a primitive 7th root of 1. Then $\mathbb{Q}(\omega)$ is a Galois extension of $\mathbb{Q}$ with degree 6 and abelian Galois group G of degree 6. Complex conjugation γ is an element of order 2 of G, and its fixed field F will be a Galois extension of $\mathbb{Q}$ of degree 3 (Galois because all subgroups of G are normal). Since $\omega + \gamma(\omega) \in F - \mathbb{Q}$, we see that $\mathbb{Q}(\omega + \gamma(\omega))$ is a Galois extension of degree 3 over $\mathbb{Q}$. We conclude that $\mathbb{Q}(\cos(2\pi/7))$ is a Galois extension of $\mathbb{Q}$. If K is any such field, then K is the splitting field of some polynomial $f \in \mathbb{Q}[x]$. Then $K(\sqrt{2})$ is the splitting field for $(x^2-2)f$ and we see that $K(\sqrt{2})$ is a Galois extension of $\mathbb{Q}$. We cannot have $\sqrt{2} \in K$, because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[K : \mathbb{Q}] = 3$. Therefore $K(\sqrt{2})$ is a Galois extension of degree 6 over $\mathbb{Q}$; let G denote the Galois group. Since K is a Galois extension of degree 3 over $\mathbb{Q}$, we see that G has a normal subgroup of index 3, i.e. of order 2. Also $\mathbb{Q}(\sqrt{2})$ is a Galois extension of degree 2 over $\mathbb{Q}$, so G also has a normal subgroup of index 2, i.e. of order 3. It follows that G is abelian and hence isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

7. Write $\psi = \mathrm{Ind}_H^G(\chi)$. For $h \in H$, we have

$$|H|\psi(h) = \sum_{g \in G} \chi(ghg^{-1}) = |G|\chi(h)$$

because $ghg^{-1} = h$ for all $g \in G$. Therefore $\psi|_H = |G/H|\chi$. By Frobenius reciprocity, we now see that

$$(\psi, \psi)_G = (\chi, \psi|_H)_H = |G/H|(\chi, \chi)_H,$$

which proves that ψ is not irreducible when $|G/H| > 1$.

Algebra Prelim Solutions, August 2018

1. The number of Sylow 5-subgroups is congruent to 1 mod 5 and divides 99, so if G does not have a normal Sylow 5-subgroup, it has 11 Sylow 5-subgroups and hence 44 elements of order 5. The number of Sylow 11-subgroups is congruent to 1 mod 11 and divides 45, so if G does not have a normal subgroup of order 11, it has 45 subgroups of order 11 and hence 450 elements of order 11. If G does not have a normal Sylow 3-subgroup, then there are at least 10 elements of order a power of 3. We now see that G has at least $44+450+10=504>495$, too many elements, and it now follows that G has normal Sylow p-subgroup for $p=3$, or 5, or 11, as required.

   If G does not have a normal Sylow 3-subgroup, then it has either a normal Sylow 5-subgroup or a normal Sylow 11-subgroup. Suppose G has a normal Sylow 5-subgroup A. Then G/A is a group of order 99, and therefore G/A has a normal subgroup B/A of order 9, because the number of Sylow 3-subgroups in a group of order 99 is 1. Since $|B|=45$, the number of Sylow 3-subgroups of B is 1 and we deduce that B has a characteristic subgroup C of order 9. We conclude that $C \lhd G$ as required. On the other hand if G has a normal Sylow 11-subgroup D, then G/D is a group of order 45 which has a normal subgroup E/D of order 9. Then E is a group of order 99 and the number of Sylow 3-subgroups is 1, consequently E has a characteristic subgroup F of order 9. It follows that G has a normal subgroup F of order 9 as required and the proof is complete.

2. Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n. We will show that $I=(f)$. If this is not the case, then we may choose $g \in I \setminus (f)$ with smallest possible degree. Clearly $g \neq 0$ and therefore $\deg(g) \geq n$, so we may write $g = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ where $m = \deg(g)$ and $a_m \neq 0$. Then $g - a_m f \in I$ and has degree strictly less than m, so we have a contradiction and the result is proven.

3. To show that $\mathbb{Q}/\mathbb{Z} \otimes I = 0$, it will be sufficient to show that ever simple tensor $x \otimes y = 0$. Choose $n \in \mathbb{N}$ such that $nx = 0$. Since I is injective, we know that $nI = I$, so there exists $z \in I$ such that $nz = y$. Then

$$x \otimes y = x \otimes nz = nx \otimes z = 0$$

   as required.

4. By the structure theorem for finitely generated modules over a PID, invariant factor form, we may write

$$M = R^d \oplus R/Rt_1 \oplus \cdots \oplus R/Rt_n$$

where $t_1|t_2|\ldots|t_n \neq 0$. Here $T := R/Rt_1 \oplus \cdots \oplus R/Rt_n$ is the torsion submodule of M. First suppose $C \cong R$. Then M is not a torsion module, so $d \geq 1$ and we may write $M = R \oplus S$, where $S = R^{d-1} \oplus T$. Then $M/S \cong R$ and it follows that we have an epimorphism $M \twoheadrightarrow C$.

Now suppose $C \ncong R$. Then C is a torsion module, so $C \subseteq T$. Since $t_n T = 0$, we see that $t_n C = 0$ and we deduce that $C \cong R/sR$ where $s|t_n$. Since there exists an R-epimorphism $R/t_nR \twoheadrightarrow R/sR$ and R/t_nR is a direct summand of M, we deduce that there exists an R-epimorphism $M \twoheadrightarrow C$, which completes the proof.

5. (a) Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Note that G has a subgroup H of order 10, for example the normalizer of a Sylow 5-subgroup, because the number of Sylow 5-subgroups is 6. Let F denote the fixed field of H. Then $[F : \mathbb{Q}] = 6$ and by the primitive element theorem, $F = \mathbb{Q}(p)$ for some $p \in F$. Let f denote the minimal polynomial of p over $\mathbb{Q}$. Then f is irreducible, $\deg f = 6$, and the splitting field for f is a Galois extension of $\mathbb{Q}$ contained in K. Since A_5 is simple, the only Galois extensions of $\mathbb{Q}$ contained in K are $\mathbb{Q}$ and K, and we deduce that K is the splitting field of f.

   (b) Complex conjugation is an element γ of G, because K is a Galois extension of $\mathbb{Q}$. The order of γ is 2, because K is not contained in the real numbers, and the fixed field of γ is R. Therefore $[K : R] = 2$ and we deduce that $[R : \mathbb{Q}] = 30$.

   (c) By considering its action on the roots of f, we get an embedding of G into S_6. If γ is an odd permutation, then the even permutations yield a subgroup of index 2 in G, which is not possible because G is simple. It follows that γ is an even permutation of order 2, so it must be a product of two 2-cycles. We deduce that f has exactly two real roots.

   (d) From (c), let a, b be the two real roots of f. Then $\mathbb{Q}(a,b) \subseteq R$. Since $6|[\mathbb{Q}(a,b) : \mathbb{Q}]$ and $[R : \mathbb{Q}] = 30$, we see that either $[\mathbb{Q}(a,b) : \mathbb{Q}] = 6$ or $[\mathbb{Q}(a,b) : \mathbb{Q}] = 30$. If the latter is true, then we must have $R = \mathbb{Q}(a,b)$ as required. On the other hand if $[\mathbb{Q}(a,b) : \mathbb{Q}] = 6$, then the corresponding

subgroup for $\mathbb{Q}(a,b)$ has order 10 in G and therefore must contain a 5-cycle σ. But then σ can only fix one root and we have a contradiction.

6. Let A be the given matrix. The characteristic polynomial f of A must be x^3+x^2+ax+1, where $a=0$ or 1. First suppose $a=0$. Then $f(x)\neq 0$ for $x=0$ or 1 and we see that f has no linear factor. It follows that f is irreducible and it we deduce that the rational canonical form for A is the companion matrix for x^3+x^2+1, that is $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

   Now suppose $a=1$. Then $f(x)=(x+1)^3$ and we see that there are three possibilities for the invariant factors, namely $\{(x+1)^3\}$, $\{(x+1)^2,(x+1)\}$ and $\{x+1,x+1,x+1\}$. The corresponding rational canonical forms are

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

   Thus there are four possible rational canonical forms, as described above.

7. Representatives for the conjugacy classes for A_4 are (1), (1 2 3), (1 3 2) and (1 2)(3 4). The sizes of the conjugacy classes are 1, 4, 4 and 3 respectively. Let V denote the Sylow 2-subgroup of A_4, a normal subgroup of order 4 consisting of 1 and the fourth conjugacy class above. Then A_4/V is a group of order 3, so it has 3 one-dimensional representations, and hence A_4 has 3 one-dimensional representations. Since A_4 has 4 conjugacy classes, it has 4 irreducible representations. Thus A_4 has one more irreducible representation, which will have degree 3, because the sum of the squares of the degrees of the irreducible representations of A_4 is $|A_4|=12$. Let ι denote the trivial character, let α,β denote the two other degree 1 characters, and let χ denote the irreducible degree 3 character. Let $\omega=e^{2\pi i/3}=(-1+i\sqrt{3})/2$ denote a primitive cube root of 1. Then the character table is

Class Size	1	4	4	3
Class Rep	1	(1 2 3)	(1 3 2)	(1 2)(3 4)
ι	1	1	1	1
α	1	ω	ω^2	1
β	1	ω^2	ω	1
χ	3	0	0	-1

The character χ is derived from the rest of the character table and the orthogonality relations.

Algebra Prelim Solutions, January 2019

1. Let G be a group of order 992. The number of Sylow 31-subgroups is congruent to 1 mod 31 and divides 32 and is therefore 1 or 32. First suppose G has 1 Sylow 31-subgroup N. Then $N \lhd G$ and G/N is a group of order 32. Since a nontrivial p-group has nontrivial center, we see that G/N has a central element of order 2 and therefore it has a normal subgroup M/N of order 2, where $M \lhd G$, by the subgroup correspondence theorem. Then M is a normal subgroup of order 62.

   Now suppose that the number of Sylow 31-subgroups is 32. Then the number of elements of order 31 is $32 \cdot 30 = 960$. It follows that G has at most 32 elements that are a power of 2. Let H be a Sylow 2-subgroup of G. Then H has 32 elements that are a power of 2. If K is another Sylow 2-subgroup, then there exists $k \in K \setminus H$, and since k has order a power of 2, we have that G has a least 33 elements that have order a power of 2. This means that G has at least $960 + 33 = 993 > 992$ elements, a contradiction. Therefore G has only one Sylow 2-subgroup and it follows that $H \lhd G$. This completes the proof.

2. Let A denote the set of prime ideals of R. Since $R \neq 0$, it has maximal ideals. Furthermore every maximal ideal is a prime ideal, consequently $A \neq \emptyset$. Partially order the prime ideals of A by reverse inclusion; that is $P \leq Q$ means $Q \subseteq P$. Suppose $\{P_j \mid j \in J\}$ is a chain in A (where J is an indexing set). Let $Q = \bigcap_j P_j$. Then Q is certainly an ideal of R (the intersection of ideals is always an ideal), so we need to check that it is prime. Suppose $a, b \in R \setminus Q$. Then $a \notin P_j$ and $b \notin P_k$ for some $j, k \in J$. Since $\{P_j\}$ is a chain, without loss of generality we may assume that $P_j \subseteq P_k$. Then $a, b \notin P_j$ and since P_j is a prime ideal, we deduce that $ab \notin P_j$ and hence $ab \notin Q$. Therefore $Q \in A$ and is an upper bound for the chain. We conclude by Zorn's lemma that A has maximal elements. This means that R has minimal prime ideals with respect to inclusion.

3. Suppose R is not a field. Then R has a nonzero maximal ideal M. Since R/M is irreducible, it is free a free R-module by hypothesis. Choose $m \in M \setminus 0$ and $x \in R \setminus M$. Since R/M is free, we see that $m(x+M) \neq 0$ in R/M. On the other hand $m(x+M) = mx + M = 0$ because M is an ideal, a contradiction, and the result follows.

4. Suppose first that $\dim_k M < \infty$. If N is a proper submodule of N, then $\dim_k N < \dim_k M$ and we cannot have $N \cong M$. This proves the "only if" part of the statement.

   Now suppose $\dim_k M = \infty$. We use the structure theorem for finitely generated modules over the PID $k[x]$ to write $M \cong k[x]^n \bigoplus_{i=1}^d k[x]/(f_i)$, where the f_i are monic polynomials with positive degree, and n and d are nonnegative integers. Since $\dim_k k[x]/(f_i) < \infty$, this implies that $n > 0$ and therefore we may write $M \cong k[x] \oplus L$ for some $k[x]$-module L. Since $xk[x]$ is a proper $k[x]$-submodule of $k[x]$ and $xk[x] \cong k[x]$, we see that $xk[x] \oplus L$ is a proper submodule of $k[x] \oplus L$ and $xk[x] \oplus L \cong k[x] \oplus L$. The result follows.

5. Let G denote the automorphism group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Since α and β are roots of the same irreducible polynomial f, there is an isomorphism $\theta\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. Thus $\theta \in G$ and therefore $G \neq 1$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f$, because f is irreducible, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, a prime, and it follows that the fixed field of G is $\mathbb{Q}$. We conclude that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$.

6. (a) Let $a, b \in K$ and $c \in k$. Then $\theta(a+b) = \theta a + \theta b$ by Freshman's dream, and $\theta(ca) = \theta c \theta a = c\theta a$ because $\theta c = c$. This proves that θ is a k-linear map.

   (b) Let $\iota\colon K \to K$ denote the identity map. Note that $\theta^n(a) = a^{p^n}$. Since $a^{p^n} = a$ for all $a \in K$, we see that $\theta^n = \iota$ and we deduce that the minimal polynomial of θ divides $X^n - 1$.

   (c) Since $n \mid p-1$, we see that the roots of $X^n - 1$ are a subset of the roots of $X^{p-1} - 1$ (including multiplicities). However the roots of $X^{p-1} - 1$ are precisely the $p-1$ nonzero elements of k. Therefore minimal polynomial has distinct roots, all lying in k. It follows that θ is diagonalizable over k.

7. S_3 has 3 conjugacy classes with representatives (1), $(1\ 2)$ and $(1\ 2\ 3)$. It has two one-dimensional characters, namely the trivial character, which we shall denote by χ_1, and the sign of a permutation, which we shall denote by χ_2. Since there are 3 conjugacy classes, there are three irreducible characters; we'll call the third irreducible character χ_3. This character can be derived from the orthogonality relations. Therefore character table for S_3 is

Class Size	1	3	2
Class Rep	1	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The character table for $\mathbb{Z}/2\mathbb{Z}$ is

Class Size	1	1
Class Rep	0	1
ψ_1	1	1
ψ_2	1	-1

The conjugacy classes for $S_3 \times \mathbb{Z}/2\mathbb{Z}$ are of the form $\mathscr{S} \times \mathscr{T}$, where $\mathscr{S}$ is a conjugacy class for S_3 and $\mathscr{T}$ is a conjugacy class for $\mathbb{Z}/2\mathbb{Z}$. Thus in particular $S_3 \times \mathbb{Z}/2\mathbb{Z}$ has $3*2=6$ conjugacy classes. We get the six irreducible representations from taking the tensor product of irreducible representations of S_3 and $\mathbb{Z}/4\mathbb{Z}$, namely the representations $\chi_i \otimes \psi_j$, which have characters $\chi_i \psi_j$.

Class Size	1	1	3	3	2	2
Class Rep	((1), 0)	((1), 1)	((1 2), 0)	((1 2), 1)	((1 2 3), 0)	((1 2 3), 1)
$\chi_1 \otimes \psi_1$	1	1	1	1	1	1
$\chi_1 \otimes \psi_2$	1	-1	1	-1	1	-1
$\chi_2 \otimes \psi_1$	1	1	-1	-1	1	1
$\chi_2 \otimes \psi_2$	1	-1	-1	1	1	-1
$\chi_3 \otimes \psi_1$	2	2	0	0	-1	-1
$\chi_3 \otimes \psi_2$	2	-2	0	0	-1	1

Algebra Prelim Solutions, August 2019

1. Let G be a simple group of order 4860. The number of Sylow 3-subgroups is congruent to 1 mod 3 and divides 20, so if G does not have a normal Sylow 3-subgroup, it has 4 or 10 Sylow 3-subgroups. If there are 4 Sylow 3-subgroups, then G will be isomorphic to a subgroup of A_4 which has order 12, which is clearly not possible because $12 < 4860$. Therefore G must have 10 Sylow 3-subgroups and then G will be isomorphic to a subgroup of A_{10}. This is not possible because $3^5 \mid 4860$, but the largest power of 3 dividing $|A_{10}| = 10!/2$ is 4. Therefore there is no such G, as required.

2. Let $f(x) = 2x^3 + 19x^2 - 54x + 3$. If f is not irreducible, then it must have a degree one factor, which we may assume is of the form $ax+b$ where $a, b \in \mathbb{Z}$ and $(a,b) = 1$, a primitive polynomial in $\mathbb{Z}[x]$. Write $f(x) = (ax+b)g(x)$ where $g \in \mathbb{Q}[x]$. Then by Gauss's lemma, $g(x) \in \mathbb{Z}[x]$. Write $g(x) = cx^2 + dx + e$ where $c, d, e \in \mathbb{Z}$. We now equate coefficients. We have $ac = 1$, so either $a = \pm 1$ or $a = \pm 2$, and $be = 3$. Suppose $a = \pm 1$. Then ± 1 or ± 3 is a root of f, which by inspection is not the case. On the other hand if $a = \pm 2$, then $\pm 1/2$ or $\pm 3/2$ is a root of f, which again by inspection is not the case. This proves that f is irreducible in $\mathbb{Q}[x]$.

3. Define $\theta \colon S \times S \to S$ by $\theta(s,t) = st$. Note that for $s_1, s_2, t_1, t_2 \in S$ and $r \in R$,

$$\begin{aligned} \theta(s_1 + s_2, t_1) &= (s_1 + s_2)t_1 = s_1 t_1 + s_2 t_1 = \theta(s_1, t_1) + \theta(s_2, t_1), \\ \theta(s_1, t_1 + t_2) &= s_1(t_1 + t_2) = s_1 t_1 + s_1 t_2 = \theta(s_1, t_1) + \theta(s_1, t_2), \\ \theta(s_1 r, t_1) &= s_1 r t_1 = \theta(s_1, r t_1). \end{aligned}$$

   This shows that θ is an R-balanced map. Therefore θ induces a group homomorphism $\phi \colon S \otimes_R S \to S$ such that $\phi(s_1, t_1) = s_1 t_1$, in particular $\phi(1 \otimes 1) = 1 \neq 0$. It follows that $S \otimes_R S \neq 0$.

4. By the structure theorem for finitely generated modules over a PID, we may write $I = T \oplus F$ where T is the torsion submodule of I and F is a free R-module. First suppose $F \neq 0$. Then we may write $F = E \oplus R$ where E is a free module, so $I = T \oplus E \oplus R$. Since R is not a field, we may choose $r \in R \setminus 0$ which is not a unit in R. Also I is an injective R-module, so $sI = I$ and hence $sR = R$ and we have a contradiction. Therefore $F = 0$ and hence I is a torsion module. It follows there exists $s \in R \setminus 0$ such that $sI = 0$. But $sI = I$ because I is injective and we conclude that $I = 0$ as required.

5. Let $A \in \mathrm{GL}_8(\mathbb{Q})$ be an element of order 7. Then $A^7 = I$, which means that the minimal polynomial of A divides $x^7 - 1$. Now $x^7 - 1 = f(x)(x-1)$ where $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, and $f(x)$ is irreducible. Since the minimal polynomial of A is not $x-1$, we see that the minimal polynomial of A is either $f(x)$ or $x^7 - 1$. Since the characteristic polynomial has degree 8, it must be $f(x)(x-1)^2$. It follows that there is one conjugacy class of matrices in $\mathrm{GL}_8(\mathbb{Q})$ which consists of elements of order 7, namely the matrices with invariant factors $\{x^7 - 1, x - 1\}$.

6. Write $G = \mathrm{Gal}(K/\mathbb{Q})$ and $F = \mathbb{Q}(e^{2\pi i/p})$. Since $G \cong S_5$, we know that $[K : \mathbb{Q}] = |S_5| = 120$.

   (a) If f is not irreducible, then we may write $f = f_1 f_2$ where $\deg f_1, \deg f_2 \geq 1$ and $\deg f_1 + \deg f_2 = \deg f = 5$. We then have

   $$[K : \mathbb{Q}] \leq (\deg f_1)!(\deg f_2)! < 5! = 120$$

   and we have a contradiction. Therefore f is irreducible. Since an irreducible polynomial over a field of zero characteristic has distinct roots, it follows that f has 5 distinct roots.

   (b) If a is a root of f, then so is γa and it follows that γ permutes the roots of f. Also F is a cyclic extension of $\mathbb{Q}$ of degree $p-1$. The subgroup corresponding to this extension in G will be a normal subgroup of index $p-1$ in G with cyclic quotient. The only normal subgroups of G which have this property have index 1 or 2 and it follows that $p = 3$.

   (c) Since $K \not\subseteq \mathbb{R}$, we see that f must have at least one complex root. Since complex roots appear in pairs, this means that f has either 2 complex roots or 4 complex roots. Since A_5 is the unique subgroup of index 2 in G, we see that F is the fixed field of A_5. Now if f has 4 complex roots, then $\gamma \in A_5$ and hence γ fixes F, which is not the case. It follows that f has 2 complex roots and therefore fixes 3 of the roots of f.

7. Write $\psi = \mathrm{Ind}_H^G \chi$. By Frobenius reciprocity, $(\psi, \psi)_G = (\psi|_H, \chi)_H$. Since $\{1, x, x^2\}$ is a transversal for H in G, we see that for $h \in H$,

   $$\psi(h) = \chi(h) + \chi(xhx^{-1}) + \chi(x^2hx^{-2}) = 3\chi(h)$$

   and we deduce that $(\psi|_H, \chi)_H = 3$. Therefore if we write $\psi = a_1\chi_1 + \cdots + a_n\chi_n$ where $a_i \in \mathbb{N}$ and χ_i is an irreducible character for all i, then $a_1^2 + \cdots + a_n^2 = 3$ and we must have $a_i = 1$ for all i and $n = 3$. This proves the result.

Algebra Prelim Solutions, August 2020

1. Let G be a group of order $63 = 3^2 \cdot 7$. The number n_7 of Sylow 7-subgroups of G divides 9 and is congruent to 1 mod 7. Hence $n_7 = 1$ and G has a normal Sylow 7-subgroup $Q \cong \mathbb{Z}_7$. We have $G \cong P \ltimes Q$ for any Sylow 3-subgroup $P < G$.

   The group $\mathrm{Aut}(Q) \cong \mathbb{Z}_7^\times$ is cyclic of order 6. Fix a generator b of Q and let $\sigma \in \mathrm{Aut}(Q)$ be the element of order 3 such that $\sigma(b) = b^2$. Since $P \cong \mathbb{Z}_9$ or $P \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, any homomorphism $P \to \mathrm{Aut}(Q)$ has image in $\langle \sigma \rangle$.

   We deduce that there exist exactly 4 non-isomorphic groups of order 63: the abelian groups $\mathbb{Z}_9 \times \mathbb{Z}_7$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$, and two non-abelian semi-direct products $\mathbb{Z}_9 \ltimes \mathbb{Z}_7$ and $(\mathbb{Z}_3 \times \mathbb{Z}_3) \ltimes \mathbb{Z}_7$. The various possibilities for the latter are seen to be isomorphic by suitably changing generators. (For example, if $\mathbb{Z}_9 \ltimes \mathbb{Z}_7$ is generated by a, b such that $a^9 = b^7 = e$ and $aba^{-1} = b^2 = \sigma(b)$, then in terms of the generators a^2, b we have $a^2ba^{-2} = b^4 = \sigma^2(b)$, corresponding to the other non-trivial homomorphism $P \to \mathrm{Aut}(Q)$ in the case $P \cong \mathbb{Z}_9$.)

2. We know that A is similar to matrix in Jordan canonical form, with nonzero eigenvalues (since A is invertible). Without loss of generality, we may assume that A is an $n \times n$ Jordan block matrix with eigenvalue $\mu \neq 0$.

   Consider a single $n \times n$ Jordan block J with eigenvalue $\lambda \neq 0$ on the diagonal and 1 on the superdiagonal. Its square J^2 has λ^2 on the diagonal, 2λ on the superdiagonal, 1 on the next diagonal, and all other entries 0. In particular, one has $(J^2 - \lambda^2 I)^n = 0$ and no smaller power of $x - \lambda^2$ annihilates J^2. Thus the Jordan canonical form of J^2 also consists of a single block, i.e., J^2 is similar to a $n \times n$ Jordan block with eigenvalue λ^2.

   Now pick $\lambda \in \mathbb{C}$ so that $\lambda^2 = \mu$. By the previous paragraph, we have $PJ^2P^{-1} = A$ for some invertible matrix P. Then $A = B^2$ for $B = PJP^{-1}$.

3. If A and B are both free, then so is $A \otimes_R B$. If either A or B is 0, then $A \otimes_R B$ is also 0 and hence free.

   Suppose A and B are both nonzero, but not both free. Without loss of generality, we may assume that A has an elementary divisor p^i. If the free part of B is nonzero, then $A \otimes_R B$ contains a (torsion) submodule isomorphic to $R/(p^i) \otimes_R R \cong R/(p^i)$ and therefore cannot be free. Thus, in order

for $A \otimes_R B$ to be free, B must be a torsion module. But then, for the same reason, A must also be a torsion module.

Assuming A and B are nonzero torsion modules, the elementary divisors of $A \otimes_R B$ are determined from those of A and B by using the bilinearity of the tensor product and the isomorphism $R/I \otimes_R R/J \cong R/(I+J)$ (or by direct arguments), which gives

$$R/(p^i) \otimes_R R/(p^j) \cong R/(p^{\min\{i,j\}})$$
$$R/(p^i) \otimes_R R/(q^j) = 0$$

for distinct primes $p, q \in R$ and positive integers i, j. Thus, in order for $A \otimes_R B$ to be free, A and B cannot have elementary divisors for a common prime.

By the classification theorem, we conclude that $A \otimes_R B$ is free if and only if one of the following holds:

- one of A, B is 0
- both A and B are free
- both A and B are nonzero torsion modules and they do not having elementary divisors for a common prime

4. The classification of finite abelian groups gives that the Sylow p-subgroup of A is $A(p) = \{a \in A \colon p^n a = 0\}$. A homomorphism $f \colon \mathbb{Z}/p^n\mathbb{Z} \to A$ is uniquely determined by $f(\overline{1})$, which must belong to $A(p)$. Moreover, for each $a \in A(p)$, since $p^n a = 0$, there exists unique such f with $f(\overline{1}) = a$, by the First Isomorphism Theorem. In other words, the map sending $f \in \mathrm{Hom}(\mathbb{Z}/p^n\mathbb{Z}, A)$ to $f(\overline{1}) \in A(p)$ is a bijection. This map is a group isomorphism, since $f_1 + f_2 \mapsto (f_1 + f_2)(\overline{1}) = f_1(\overline{1}) + f_2(\overline{1})$.

5. (a) Let $\alpha = \sqrt[3]{4} \in \mathbb{R}$, $\beta = \alpha\omega$, $\gamma = \alpha\omega^2$ be the roots of $x^3 - 4$, where $\omega = e^{2\pi i/3}$ is a primitive 3rd root of unity. We have $E = \mathbb{Q}(\alpha, \omega)$.

   We claim that $E/\mathbb{Q}$ has degree 6. We know that $[E \colon \mathbb{Q}] \leq 3! = 6$. The polynomial $x^3 - 4$ is irreducible over $\mathbb{Q}$, since it has degree 3 and no rational roots (since $\pm 1, \pm 2, \pm 4$ are not roots). The minimal polynomial of ω is $x^2 + x + 1$. Since E contains α and ω, its degree $[E \colon \mathbb{Q}]$ must be divisible by 2 and 3, hence by 6. Therefore $[E \colon \mathbb{Q}] = 6$.

   The action of $G = \mathrm{Gal}(E/\mathbb{Q})$ on α, β, γ gives an injective homomorphism $G \to S_3$. Since $|G| = 6$, it must be an isomorphism $G \cong S_3$.

By the Galois correspondence, $E/\mathbb{Q}$ has one intermediate field for each subgroup of S_3, of which there are 6. Thus

$$\mathbb{Q}, \mathbb{Q}(\omega), \mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\gamma), E$$

are all intermediate fields of $E/\mathbb{Q}$. (These are the fixed fields of the subgroups $S_3, \langle(123)\rangle, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle e\rangle$, respectively, where we identify α with 1, β with 2, and γ with 3.)

(b) It suffices to find $\theta \in E$ whose stabilizer in G is trivial. One checks that $\theta = \alpha + \omega$ has this property:

$$\begin{aligned}
\alpha + \omega &\overset{(12)}{\longmapsto} \beta + \omega^{-1} = \alpha\omega - \omega - 1 \\
\alpha + \omega &\overset{(13)}{\longmapsto} \gamma + \beta/\gamma = \alpha\omega^2 + \omega^{-1} = \alpha(-\omega - 1) - \omega - 1 \\
\alpha + \omega &\overset{(23)}{\longmapsto} \alpha + \gamma/\alpha = \alpha - \omega - 1 \\
\alpha + \omega &\overset{(123)}{\longmapsto} \beta + \omega = \alpha\omega + \omega \\
\alpha + \omega &\overset{(132)}{\longmapsto} \gamma + \omega = \alpha\omega^2 + \omega
\end{aligned}$$

Here we use that $\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\}$ is a $\mathbb{Q}$-basis of E to see that none of these images are equal to $\alpha + \omega$.

6. (a) We know $\mathscr{S}$ is not empty, because the zero ideal belongs to $\mathscr{S}$. Let $I_1 \subset I_2 \subset \cdots$ be a chain in $\mathscr{S}$. The union $I = \bigcup_{n=0}^{\infty} I_n$ is an ideal of R and $a^k \notin I$ for all $k \geq 0$. Hence I belongs to $\mathscr{S}$ and is an upper bound for the chain. We have verified the conditions of Zorn's lemma.

(b) Let P be a maximal element of $\mathscr{S}$. Then $a \notin P$. We will show that P is a prime ideal of R. Suppose $xy \in P$ for some $x, y \in R$, but $x, y \notin P$. Then the ideals $(x) + P$ and $(y) + P$ strictly contain P, and therefore do not belong to $\mathscr{S}$. Hence $a^k \in (x) + P$ and $a^l \in (y) + P$ for some $k, l \geq 0$. But then $a^{k+l} \in (xy) + P = P$, which is a contradiction, since $P \in \mathscr{S}$.

7. (a) We apply the orbit-stabilizer theorem. We have $hxk^{-1} = x$ if and only if $h = xkx^{-1} \in H \cap xKx^{-1}$. Hence the stabilizer of x has $|H \cap xKx^{-1}|$ elements, and the orbit of x has $|H \times K|/|H \cap xKx^{-1}|$ elements.

(b) The orbit through the identity is $HeH = H$, which has $|H| = q(q-1)^2$ elements. Taking any $s \notin H$, e.g., $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we find that $|H \cap$

$|sHs^{-1}| = (q-1)^2$ and hence, by (a), the orbit through s has size $q^2(q-1)^4/(q-1)^2 = q^2(q-1)^2$. Since $(q^2+q)(q-1)^2 = q(q+1)(q-1)^2 = |G|$ we are done.