1. (Aug-12.1) Let $p$ be a prime. For any finite group $G$, let $\mathbb{B}(G)$ be the subgroup of $G$ generated by all Sylow $p$-subgroups of $G$.

(a) Show that $\mathbb{B}(G)$ is the unique normal subgroup of $G$ minimal with respect to having its index not divisible by $p$.

(b) Let $L$ be normal in $G$. Show that $\mathbb{B}(L)$ is normal in $G$ and $\mathbb{B}(L) = \mathbb{B}(G)$ if $|G : L|$ is not divisible by $p$.

(c) Let $H$ be a subgroup of $G$ with $|G : H| = p$. If $L$ is the largest normal subgroup of $G$ contained in $H$, prove that $|H : L|$ is not divisible by $p$ and deduce that $\mathbb{B}(H)$ is normal in $G$.

Solution: Let $p^n$ be the largest power of $p$ dividing the order of $G$.

a) First observe that $\mathbb{B}(G)$ is normal, since conjugating an element of $p$-power order yields another element of $p$-power order, hence the same holds for the product of such elements. Now if $H$ is any normal subgroup of $G$ whose index is not divisible by $p$, its order is divisible by $p^n$, hence it contains a Sylow $p$-subgroup of $G$. Since all Sylow $p$-subgroups of $G$ are conjugate, we see that $H$ contains all of them, hence contains $\mathbb{B}(G)$.

b) Let $h = g_1 \cdots g_k \in \mathbb{B}(L)$, where each $g_i$ is contained in a Sylow-$p$ subgroup of $L$. Any $G$-conjugate of $g_i$ lies in $L$ since $L$ is normal, and each of the $g_i$ is therefore sent to another Sylow-$p$ element of $L$: thus by the same argument as in part (a), we see $ghg^{-1} \in \mathbb{B}(L)$, hence $\mathbb{B}(L)$ is normal in $G$. If $|G : L|$ is not divisible by $p$, then $p^n$ divides $|L|$ hence $L$ contains a Sylow $p$-subgroup of order $p^n$ which is necessarily a Sylow $p$-subgroup of $G$. Then as in part (a), $L$ contains all Sylow $p$-subgroups of $G$ hence contains $\mathbb{B}(G)$; then by the minimality property of (a) we get $\mathbb{B}(G) = \mathbb{B}(L)$. (Alternatively, one could observe that the $p$-Sylow subgroups of $G$ are the same as those of $L$.)

c) First, we observe that any automorphism of $G$ permutes the Sylow $p$-subgroups, hence fixes $\mathbb{B}(G)$ — thus, $\mathbb{B}(G)$ is characteristic in $G$. Now, $\mathbb{B}(G)$ is normal in $G$ and contains all $p$-Sylow subgroups of $G$ (hence of $H$, since every $p$-subgroup of $G$ is contained in some $p$-Sylow subgroup); then $\mathbb{B}(G) \cap H$ is normal in $G$ (since $\mathbb{B}(G)$ is characteristic) and contains a $p$-Sylow subgroup of $H$. Hence $L$ hence $\mathbb{B}(G) \cap H$ has order divisible by $p^{n-1}$, so $|H : L|$ is not divisible by $p$. For the final statement, we know that $\mathbb{B}(H)$ is normal in $H$, and by part (b) we know $\mathbb{B}(L) = \mathbb{B}(H)$ so $\mathbb{B}(L)$ is normal in $L$. Since $L$ is normal in $G$ and $\mathbb{B}(G)$ is characteristic in $L$, we conclude $\mathbb{B}(H) = \mathbb{B}(L)$ is normal in $G$.

2. (Aug-12.2) Let $F$ be a field, $R = F[x, y]$, and $I = (x)$.

(a) Prove that $I/I^2$ is infinite-dimensional as an $F$-vector space.

(b) Let $S \subset R$ be the subring $S = F + I$, so that $I$ is also an ideal of $S$. Show that $I$ is not finitely-generated as an ideal of $S$.

(c) Let $M$ be a maximal ideal of $R$ and $\theta : R \rightarrow R/M$ be the projection map. Then $\theta(S)$ is a ring with $\theta(F) \subseteq \theta(S) \subseteq \theta(R)$. Discuss the nature of the extension $\theta(F) \subseteq \theta(R)$, prove that $\theta(S)$ is a field, and conclude that $M \cap S$ is a maximal ideal of $S$.

Solution:

a) The elements of $I$ are of the form $x \cdot p(x, y)$ for a polynomial $p(x, y)$. We can write any such element in the form $x \cdot q(y) + x^2r(x, y)$, the image of which in $I^2$ is $x \cdot q(y)$. Thus we see that $I/I^2$ is generated as a vector space by $x$, $xy$, $x^2y$, $xy^2$, $x^3y$, and is infinite-dimensional.

b) If $I$ were finitely-generated as an ideal of $S$, then $I/I^2$ would be a finitely-generated ideal of $S/I^2$. But the elements of $S/I^2$ are of the form $c + xp(y)$ where $c \in F$ and $p(y) \in F[y]$, and the only ones in $I/I^2$ are those with $c = 0$. But then the product of any two terms $xp(y)$ and $xq(y)$ is zero, so $I/I^2$ has trivial ring structure. The non-finite-generation then follows from part (a), since then finite generation of $I/I^2$ as a ring is equivalent to finite generation as an $F$-vector space. (Or, explicitly: if there are only finitely many generators, then it is not possible to obtain the term $x \cdot y^n$ where $n$ is any integer larger than any of the $y$-degrees of the generators’ images in $I/I^2$. )
c) \( \theta(R) \cong R/M \) is a field extension of \( \theta(F) \); since \( R \) is Noetherian, this field extension is of finite degree. If \( x \in M \) then \( \theta(S) = \theta(F) \) is a field; otherwise, assume \( x \not\in M \), so that \( x \) is invertible in \( R/M \). We also see that \( S + M = F + I + M \), and \( I + M \) is an ideal of \( R \) containing \( M \), hence since \( M \) is maximal it is either equal to \( M \) or to \( R \); thus \( S + M \) is either \( F + M \) or \( F + R \), so we see \( \theta(S) \) is either \( \theta(F) \) or \( \theta(R) \), hence is a field. By the first isomorphism theorem for rings, we conclude that \( S/(M \cap S) \cong \theta(S) \) is a field, so \( M \cap S \) is a maximal ideal of \( S \).

3. (Aug-12.3):

(a) Suppose \( K, L \subseteq \mathbb{C} \) are Galois over \( \mathbb{Q} \). Show that \( E = KL \) is Galois over \( \mathbb{Q} \).

(b) If additionally \( [K : \mathbb{Q}] \) and \( [L : \mathbb{Q}] \) are coprime, show that \( \text{Gal}(E/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \), and deduce \( |E : \mathbb{Q}| = |K : \mathbb{Q}| \cdot |L : \mathbb{Q}| \).

(c) Prove there is a subfield \( F \) of \( \mathbb{C} \), Galois over \( \mathbb{Q} \), with \( [F : \mathbb{Q}] = 55 \).

Solution:

(a) This is standard: first, observe that \( K \cap L \) is Galois over \( \mathbb{Q} \), since if \( p(x) \in \mathbb{Q}[x] \) is irreducible with a root in \( K \cap L \), then since \( K/\mathbb{Q} \) is Galois all its roots lie in \( K \); similarly all its roots lie in \( L \), so all its roots lie in \( K \cap L \). Now \( KL \) is also Galois over \( \mathbb{Q} \); if \( K \) is the splitting field of \( f(x) \) and \( L \) is the splitting field of \( g(x) \), then \( KL \) is the splitting field of the polynomial \( fg/\text{gcd}(f, g) \).

(b) Continuing part (a): we claim that \( \text{Gal}(KL/\mathbb{Q}) \) is the subgroup \( H \) of \( \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \) where the actions in both components agree on \( K \cap L \) - to prove this, observe that the map \( \text{Gal}(KL/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \) via \( \sigma \mapsto (\sigma \vert_K, \sigma \vert_L) \) is well-defined, and the kernel is the set of maps which are trivial on \( K_1 \) and \( K_2 \) hence on the composite. The image lies in \( H \), so we need only verify that its order agrees with that of \( H \). We have \( |H| = |\text{Gal}(K/\mathbb{Q})| \cdot |\text{Gal}(L/K \cap L)| \) since for every \( \sigma \in \text{Gal}(K/\mathbb{Q}) \) there are \( |\text{Gal}(L/K \cap L)| \) elements whose restrictions to \( K \cap L \) agree with \( \sigma \). We then see that \( |H| = |\text{Gal}(K/\mathbb{Q})| \cdot |\text{Gal}(L/K \cap L)| = |\text{Gal}(K/\mathbb{Q})| \cdot \frac{|\text{Gal}(L/K \cap L)|}{|\text{Gal}(KL/\mathbb{Q})|} = |\text{Gal}(KL/\mathbb{Q})| \).

Then for the deduction in the problem, we just need to observe that given our assumptions, \( K \cap L = \mathbb{Q} \); its degree over \( \mathbb{Q} \) divides both \( [K : \mathbb{Q}] \) and \( [L : \mathbb{Q}] \), so it must be \( 1 \) since these degrees are coprime. (We could of course shorten the original proof by incorporating this assumption.)

(c) We know that \( \mathbb{Q}(\zeta_{23}) \) is cyclic Galois of degree \( \phi(23) = 22 \) over \( \mathbb{Q} \), and \( \mathbb{Q}(\zeta_{11}) \) is cyclic Galois of degree \( \phi(11) = 10 \) over \( \mathbb{Q} \). Then we can take fixed subfields of degrees 11 and 5, which are also Galois and cyclic. By part (b) their compositum is cyclic Galois over \( \mathbb{Q} \) of degree 55.

c-alt) Since 221 is prime and 1 mod 55, then \( \mathbb{Q}(\zeta_{221}) \) is cyclic Galois of order 220, and hence has a subfield of degree 55 that is Galois over \( \mathbb{Q} \).

4. (Aug-12.4): Let \( V \) be an \( n \)-dimensional \( K \)-vector space and \( T : V \to V \).

(a) Suppose there exists \( v \in V \) such that \( V \) is spanned by \( v, T v, T^2 v, \ldots \). Prove that the minimal polynomial of \( T \) equals the characteristic polynomial of \( T \).

(b) As a partial converse, suppose the characteristic polynomial of \( T \) has distinct roots in \( K \). Prove that there exists \( v \in V \) such that \( V \) is spanned by \( v, T v, T^2 v, \ldots \).

Solution:

(a) If \( m(x) \) is the minimal polynomial of \( T \), then for any vector \( w \) we know that \( m(T)w = 0 \), so in particular \( m(T)v = 0 \). But since \( v, T v, \ldots, T^{n-1} v \) are linearly independent, we see that the degree of \( m(x) \) must be \( \geq n \). But \( m(x) \) divides the characteristic polynomial, which has degree \( n \), so they must be equal since they are both monic.

(b) Let \( \lambda_1, \ldots, \lambda_n \) be the eigenvalues of \( T \) with corresponding basis of eigenvectors \( v_1, \ldots, v_n \); by the given assumptions we know that the \( v_i \) are linearly independent. We claim that \( v = v_1 + \cdots + v_n \) has the desired property: to see this, suppose that \( p(T)v = 0 \); then we see that \( 0 = p(T)v = \sum p(\lambda_i)v_i \), so since the \( v_i \) are linearly independent we see that \( p(\lambda_i) = 0 \) for each \( \lambda_i \) - now since the eigenvalues of
5. (Aug-12.5) Let $R$ be a not necessarily commutative ring with 1, such that $x^5 = x$ for every $x \in R$.

(a) Show that $J(R) = 0$.

(b) Now assume $R$ is right-Artinian. Prove that $R$ is a direct sum of division rings.

(c) Let $D$ be a division ring direct summand of $R$. If $F$ is any subfield of $D$, show that $F = \mathbb{F}_2, \mathbb{F}_3, \text{or } \mathbb{F}_5$.

(d) Deduce that $D$ above is isomorphic to $\mathbb{F}_2, \mathbb{F}_3, \text{or } \mathbb{F}_5$, and conclude that $R$ is commutative.

Solution:

a) If $y \in J$, then $1 - xy$ is a unit for all $y \in R$. But we know that $y(1 - y \cdot y^3) = 0$, so $1 - y^4$ cannot be a unit unless $y = 0$. Hence $y \not\in J$ unless $y = 0$.

b) A right-Artinian ring has a finite number of maximal right ideals $m_1, \ldots, m_k$, as otherwise $m_1, m_1\cap m_2, \ldots$ would yield an infinite decreasing chain of right ideals. Now since the Jacobson radical is the intersection of the maximal right ideals of $R$, part (a) implies that $\cap m_k = 0$. Now by the Chinese Remainder Theorem, we see that $R \cong \bigoplus (R/m_k)$, since by maximality it must be the case that $m_i + m_j = R$ for any $(i, j)$, and so $\prod m_j = \cap m_j = 0$. Finally, $R/m_k$ is a division ring.

c) Suppose $F$ is a field in which $x^5 - x = 0$ for all $x \in F$. By unique factorization we see that $|F| \leq 5$, and so $|F|$ can only be 2, 3, 4, or 5. It is then trivial to see that $|F| = 2, 3, 5$ work, but $|F| = 4$ does not work.

d) If $z \in D$ is any other element of $D$, then $F(z)$ is also commutative hence also a subfield of $D$; thus, $F(z) = F$, so $z \in F$ hence $D = F$. Thus, $R$ is a direct sum of fields hence commutative.