Answers to the Algebra Qualifying Exam
January 1991

1. Let P be a Sylow p-subgroup of G and set $N = \mathbb{N}_G(P)$. By assumption, $|G : N| = n$ and therefore the $n!$-Theorem implies that there is a homomorphism $^-: G \to \mathrm{Sym}_n$ with kernel $K \subseteq N$. We know that $\overline{PK} = PK/K$ is a Sylow p-subgroup of $\bar{G} \subseteq \mathrm{Sym_n}$. Furthermore, if $M = \mathbb{N}_G(PK)$, then the one-to-one correspondence between the subgroups of $\bar{G}$ and the subgroups of G containing K implies that $\bar{M} = \mathbb{N}_{\bar{G}}(\overline{PK})$ and that $|\bar{G} : \bar{M}| = |G : M|$. It remains to identify M. First, since $K \triangleleft G$, it is clear that $M \supseteq \mathbb{N}_G(P) = N$. Conversely, since $PK \triangleleft M$, the Frattini argument implies that $M = \mathbb{N}_M(P) \cdot PK \subseteq \mathbb{N}_G(P) = N$. Thus $M = N$ and $|\bar{G} : \bar{M}| = |G : M| = |G : N| = n$.

2. (a) This is the Nullstellensatz. Let M be a maximal ideal of the polynomial ring $S = R[x_1, x_2, \ldots, x_n]$ containing I. Then S/M is a field extension of the complex numbers R which is finitely generated as a ring extension. The Zariski Nullstellensatz implies that S/M is algebraic over R and hence $S/M = R$. In particular, under the homomorphism $\varphi: S \to S/M = R$, we have $\varphi(x_i) = a_i \in R$. Thus $\varphi = \varphi_{\mathbf{a}}$ and since $\ker \varphi = M \supseteq I$, we have $0 = \varphi_{\mathbf{a}}(I) \neq R$.

(b) Let F be the field $R/3R$. Then the nontrivial ring homomorphism $R[x] \to F[x] \to F[x]/(x^2 + 1)$ has I in its kernel. Thus $I \neq R[x]$.

If $\varphi_{\mathbf{a}}: R[x] \to R$, then since $I \supseteq 3R$, we have $\varphi_{\mathbf{a}}(I) \supseteq 3R$. Furthermore, since $\varphi_{\mathbf{a}}(I) \triangleleft R$, we must therefore have $\varphi_{\mathbf{a}}(I) = 3R$ or R. If $\varphi_{\mathbf{a}}(I) = 3R$, then $a^2 + 1 \in 3R$ so $a^2 \equiv -1$ (3). But $0^2 \equiv 0$ and $1^2 \equiv 2^2 \equiv 1$. Thus there are no possibilities for a, a contradiction, and $\varphi_{\mathbf{a}}(I) = R$.

3. (a) If $\gamma \in E$, then its minimal polynomial over F has degree dividing $|E : F| = 4$, that is 1, 2 or 4. Since the characteristic is not 2, it follows that this irreducible polynomial has a nonzero derivative and hence is separable. Thus E/F is separable and the Primitive Element Theorem implies that $E = F[\alpha]$ for some $\alpha \in E$.

(b) α^2 satisfies the quadratic $y^2 + ay + b \in F[y]$, so $|F[\alpha^2] : F| \leq 2$. Furthermore, $|F[\alpha] : F[\alpha^2]| \leq 2$. Since $|F[\alpha] : F| = 4$, we must have equality throughout and $F[\alpha^2]$ is the appropriate intermediate field.

(c) Since β satisfies a polynomial of degree 4 over F, we know that $|L : F| \leq 4!$. But $G = \mathrm{Gal}(L/F) = \mathrm{Sym}_4$ has order $4!$ so this forces L to be a Galois extension of F of degree precisely $4!$. Furthermore, E is the fixed field of a subgroup H of G of index 4. Note that Alt_4 has no subgroup of index 2. This implies first that Alt_4 is the unique subgroup of Sym_4 of index 2 and then that any subgroup of Sym_4 of index 4 is maximal. Therefore H is maximal in G and hence there is no field properly between E and F.

4. Suppose v is an eigenvector for A with eigenvalue μ. Of course, such a v exists since F is algebraically closed. Then $Av = \mu v$ so

$$A(Bv) = (BA + B)v = B(\mu v) + Bv = (\mu + 1)Bv.$$

Since B is nonsingular, Bv is therefore a (nonzero) eigenvector for A with eigenvalue $\mu + 1$.

In particular, if we set $v_i = B^{i-1}v$ and $\mu_i = \mu + i - 1$, then $v_1, v_2, \ldots, v_p$ are p eigenvectors for A with distinct eigenvalues. Thus they are linearly independent and, since

$\dim V = p$, they form a basis for V. It follows that up to a scalar multiple, these are the unique eigenvectors for A. Finally, Bv_p is an eigenvector for A with eigenvalue $\mu + p = \mu$, so $Bv_p = \lambda v_1$ for some $0 \neq \lambda \in F$.

5. (a) If $x, y \in G$, then the subgroups $\langle x \rangle$ and $\langle y \rangle$ are comparable. If say $\langle x \rangle \subseteq \langle y \rangle$, then x is a power of y and hence x and y commute. Thus G is commutative.

If $o(x) = \infty$, then $\langle x^2 \rangle$ and $\langle x^3 \rangle$ are not comparable, a contradiction. Thus all elements of G have finite order.

Finally, suppose p and q are primes with $p \mid o(x)$ and $q \mid o(y)$. Then $\langle x \rangle$ contains a subgroup X of order p and $\langle y \rangle$ has a subgroup Y of order q. But, if $q \neq p$, then X and Y are surely incomparable, a contradiction. It follows that the orders of the elements of G are all powers of the same prime p.

(b) G_n is certainly a subgroup of G. Let H be any finite subgroup of G_n. Then H is a finite abelian group of period dividing p^n. By the Fundamental Theorem of Abelian Groups, H is the direct product of cyclic factors. But any two nonidentity cyclic factors are incomparable, a contradiction. Thus H is cyclic and $|H| \leq p^n$. Since G_n is clearly the union of all its subgroups of finite order, we conclude that $|G_n| \leq p^n$.