Algebra - Fall 2009

Daren Cheng
Jesse Madnick

Last updated: September 2013

Acknowledgments & Disclaimers

Some of the solutions contained herein are my own, but many are not. I am indebted to Daren Cheng for sharing with me his solutions to several full-length exams. I'd also like to acknowledge Zev Chonoles, Fernando Shao, and my algebra professors Dan Bump and Akshay Venkatesh, all of whom patiently tolerated my many questions.

I am not exactly an algebraist. My writing style tends towards the wordy side, and my preferred proofs are rarely the most elegant ones. Still, I hope to keep these solutions free of any substantial errors. For this reason: if you notice any errors (typographical or logical), *please* let me know so I can fix it! Your speaking up would be a kindness for future students who may be struggling to make sense of an incorrect expression. I can be reached at jmadnick@math.stanford.edu.

1. Let k be a finite field of size q.

(a) Prove that the number of 2×2 matrices over k satisfying $T^2 = 0$ is q^2.

Sketch: One can use a method analogous to the solution in (b). Alternatively, a direct elementary counting argument also works (really).

(b) Prove that the number of 3×3 matrices over k satisfying $T^3 = 0$ is q^3.

Solution: Let T be a 3×3 matrix with $T^3 = 0$. Let $m_T(x) \in \mathbb{F}_q[x]$ denote the minimal polynomial of T. Since $T^3 = 0$, we have $m_T(x) \mid x^3$, so we have three cases.

Case One: $m_T(x) = x$. In this case, we have $T = 0$, so there is 1 possibility.

Case Two: $m_T(x) = x^2$. Every such matrix T is similar to the Jordan form

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

Thus, we have to compute the number of matrices that are similar to A.

Consider the action of $\mathrm{GL}_3(\mathbb{F}_q)$ on the set $M_3(\mathbb{F}_q)$ of 3×3 matrices by conjugation. The orbit of A is precisely the set of matrices that are similar to A. By the Orbit-Stabilizer Theorem,

$$|\mathrm{Orbit}(A)| = \frac{|\mathrm{GL}_3(\mathbb{F}_q)|}{|\mathrm{Stab}(A)|}.$$

Note that $|\mathrm{GL}_3(\mathbb{F}_q)| = (q^3 - 1)(q^3 - q)(q^3 - q^2)$ and $\mathrm{Stab}(A) = \{P \in \mathrm{GL}_3(\mathbb{F}_q) \colon PA = AP\}$.

If

$$P = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_q),$$

then the condition $PA = AP$ forces $a = e$ and $d = f = g = 0$, so that $|\mathrm{Stab}(A)| = q^3(q-1)^2$. Thus, $|\mathrm{Orbit}(A)| = (q^3 - 1)(q + 1) = q^4 + q^3 - q - 1$.

Case Three: $m_T(x) = x^3$. Every such matrix T is similar to the Jordan form

$$B = \begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix}$$

Thus, we have to compute the number of matrices that are similar to B.

If P is as above, then the condition $PB = BP$ forces $a = e = j$ and $b = f$ and $d = g = h = 0$, so that $|\mathrm{Stab}(B)| = q^2(q-1)$. Thus, $|\mathrm{Orbit}(B)| = q(q^3 - 1)(q^2 - 1) = q^6 - q^4 - q^3 + q$.

Conclusion: Thus, the total number of 3×3 matrices T with $T^3 = 0$ is

$$1 + (q^4 + q^3 - q - 1) + (q^6 - q^4 - q^3 + q) = q^6.$$

2. (a) Prove that if K is a field of finite degree over $\mathbb{Q}$ and $x_1, \ldots, x_n$ are finitely many elements of K, then the subring $\mathbb{Z}[x_1, \ldots, x_n]$ they generate over $\mathbb{Z}$ is not equal to K. (Hint: Show they all lie in $\mathcal{O}_K[1/a]$ for a suitable nonzero a in $\mathcal{O}_K$, where $\mathcal{O}_K$ denotes the integral closure of $\mathbb{Z}$ in K.)

Solution: Let $K/\mathbb{Q}$ be a finite extension. For each $x_i \in K$, there exists an integer $a_i \in \mathbb{Z}$ such that $a_i x_i \in \mathcal{O}_K$. Then

$$x_1, \ldots, x_n \in \mathcal{O}_K\left[\frac{1}{a_1}, \ldots, \frac{1}{a_n}\right] = \mathcal{O}_K\left[\frac{1}{a}\right],$$

where $a = \operatorname{lcm}[a_1, \ldots, a_n]$. Thus, $\mathbb{Z}[x_1, \ldots, x_n] \subset \mathcal{O}_K\left[\frac{1}{a}\right]$.

Let $p \in \mathbb{Z}$ be a prime number with $\gcd(p, a) = 1$. Then $1/p \in K$ but $1/p \notin \mathcal{O}_K\left[\frac{1}{a}\right]$. Thus, $\mathcal{O}_K\left[\frac{1}{a}\right] \subsetneq K$.

(b) Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{Z}[x_1, \ldots, x_n]$ and $F = \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{m}$. Use (a) and the Nullstellensatz to show that F cannot have characteristic 0, and then deduce that for $p = \operatorname{char}(F)$ that F is of finite degree over $\mathbb{F}_p$ (so F is actually finite).

Solution: Suppose for the sake of contradiction that F has characteristic 0. On the one hand, note that $F = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_1, \ldots, \alpha_n \in F$. On the other hand, F is a finitely-generated $\mathbb{Z}$-algebra that contains $\mathbb{Q}$, hence is a finitely-generated $\mathbb{Q}$-algebra. By the Nullstellensatz, $F/\mathbb{Q}$ is a finite extension. These two facts contradict part (a).

Thus, F has characteristic p. Let φ denote the composition $\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow F$. Since $\operatorname{char}(F) = p$, we have $(p) = \operatorname{Ker}(\varphi) = \iota^{-1}(\mathfrak{m})$, so $p\mathbb{Z}[x_1, \ldots, x_n] \subset \mathfrak{m}$. Therefore, $\mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow F$ descends to a surjective map $\mathbb{F}_p[x_1, \ldots, x_n] \twoheadrightarrow F$, so that F is a finitely-generated $\mathbb{F}_p$-algebra.

Since F is a field and a finitely-generated $\mathbb{F}_p$-algebra, the Nullstellensatz implies that $F/\mathbb{F}_p$ is a finite extension.

3. Let E be the splitting field of $f(x) = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$. Let ζ be a zero of $f(x)$, i.e. a primitive seventh root of 1.

(a) Show that $f(x)$ is irreducible over $\mathbb{Q}$. (Hint: Consider $f(y+1)$ and use Eisenstein's criterion.)

Solution: Note that $f(y+1) = \dfrac{(y+1)^7 - 1}{y} = y^6 + \dbinom{7}{6}y^5 + \ldots + \dbinom{7}{1}$. Since we have $7 \mid \binom{7}{k}$ for all $1 \leq k \leq 6$ and $7^2 \nmid \binom{7}{1}$, Eisenstein's Criterion applies.

(b) Show that the Galois group of $E/\mathbb{Q}$ is cyclic, and find an explicit generator.

Solution: Note that $E = \mathbb{Q}(\zeta)$. Consider the homomorphism

$$\begin{aligned} \psi\colon (\mathbb{Z}/7\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ a \pmod 7 &\mapsto \sigma_a\colon [\zeta \mapsto \zeta^a] \end{aligned}$$

Note that ψ is injective. Since $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta)\colon \mathbb{Q}] = \varphi(7) = 6$ and $|(\mathbb{Z}/7\mathbb{Z})^\times| = 6$, we see that ψ is an isomorphism. Thus, $\mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.

The automorphism σ_3 (or σ_5) is a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

(c) Let $\beta = \zeta + \zeta^2 + \zeta^4$. Show that the intermediate field $\mathbb{Q}(\beta)$ is actually $\mathbb{Q}(\sqrt{-7})$. (Hint: First show that $[\mathbb{Q}(\beta)\colon \mathbb{Q}] = 2$ by finding a linear dependence over $\mathbb{Q}$ among $\{1, \beta, \beta^2\}$.

Solution: Note that

$$\begin{aligned} \beta^2 + \beta + 2 &= (\zeta^2 + \zeta^4 + \zeta + 2(\zeta^3 + \zeta^5 + \zeta^6)) + (\zeta + \zeta^2 + \zeta^4) + 2 \\ &= 2(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) \\ &= 0. \end{aligned}$$

Since β is a root of $x^2 + x + 2 = 0$, we see that $\beta = -\frac{1}{2} \pm \frac{\sqrt{-7}}{2}$. Thus, $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-7})$.

(d) Let $\gamma_q = \zeta + \zeta^q$. Find (with proof) a q such that $\mathbb{Q}(\gamma_q)$ is a degree 3 extension of $\mathbb{Q}$. (Hint: use (b)). Is this extension Galois?

Solution: Consider $\gamma_6 = \zeta + \zeta^6$. Since $\mathrm{Gal}(E/\mathbb{Q})$ is abelian, every intermediate field is Galois over $\mathbb{Q}$, so $\mathbb{Q}(\gamma_6)/\mathbb{Q}$ is Galois. Let's determine $\mathrm{Gal}(E/\mathbb{Q}(\gamma_6)) \leq \{\sigma_1, \ldots, \sigma_6\}$.

Clearly $\sigma_1, \sigma_6 \in \mathrm{Gal}(E/\mathbb{Q}(\gamma_6))$. Conversely, suppose $\sigma_a \in \mathrm{Gal}(E/\mathbb{Q}(\gamma_6))$. Then $\sigma_a\gamma_6 = \gamma_6$, so $\zeta^a + \zeta^{-a} = \zeta + \zeta^6$. If $a \neq 1, 6$, then this gives a linear dependence among the distinct basis elements $\zeta, \zeta^6, \zeta^a, \zeta^{-a}$, which is impossible. Thus, $\mathrm{Gal}(E/\mathbb{Q}(\gamma_6)) = \{\sigma_1, \sigma_6\}$.

Therefore,

$$\mathrm{Gal}(\mathbb{Q}(\gamma_6)/\mathbb{Q}) \cong \frac{\mathrm{Gal}(E/\mathbb{Q})}{\mathrm{Gal}(E/\mathbb{Q}(\gamma_6))} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{\{\sigma_1, \sigma_6\}} \cong \mathbb{Z}/3\mathbb{Z}.$$

Hence, $[\mathbb{Q}(\gamma_6)\colon \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\gamma_6)/\mathbb{Q})| = 3$.

4. Let G be a nontrivial finite group and p be the smallest prime dividing the order of G. Let H be a subgroup of index p. Show that H is normal. (Hint: If H isn't normal, consider the action of G on the conjugates of H.)

Solution: Since $H \leq N_G(H) \leq G$ and $|G\colon H| = p$, we have either $N_G(H) = G$ or $N_G(H) = H$. In the first case, H is normal, and we're done.

Suppose, then, for the sake of contradiction, that $N_G(H) = H$. In this case, the number of conjugates of G is equal to $|G\colon N_G(H)| = |G\colon H| = p$. Let $T = \{g_1 H g_1^{-1}, \ldots, g_p H g_p^{-1}\}$ denote the set of conjugates of H, where we set g_1 as the identity element.

Consider the action by conjugation of G on the set T. This gives a map

$$\begin{aligned} \pi\colon G &\to \mathrm{Perm}(T) \cong S_p \\ g &\mapsto [g_i H g_i^{-1} \mapsto g g_i H g_i^{-1} g^{-1}] \end{aligned}$$

Note that the stabilizer of an element $gHg^{-1} \in T$ is

$$\mathrm{Stab}(gHg^{-1}) = g\,\mathrm{Stab}(H)\,g^{-1} = gN_G(H)g^{-1} = gHg^{-1},$$

so that

$$\mathrm{Ker}(\pi) = \bigcap_{i=1}^{p} \mathrm{Stab}(g_i H g_i^{-1}) = \bigcap_{i=1}^{p} g_i H g_i^{-1} \subset H.$$

Therefore, $|G\colon \mathrm{Ker}(\pi)| = |G\colon H||H\colon \mathrm{Ker}(\pi)| = p\,|H\colon \mathrm{Ker}(\pi)|$. Since we also have $|G\colon \mathrm{Ker}(\pi)| = |\mathrm{Im}(\pi)| \mid p!$, it follows that

$$|H\colon \mathrm{Ker}(\pi)| \mid (p-1)!$$

Since all prime divisors of $(p-1)!$ are strictly less than p, it follows that any prime divisor of $|H\colon \mathrm{Ker}(\pi)|$ must be strictly less than p. On the other hand, since $|H\colon \mathrm{Ker}(\pi)| \mid |G|$, the minimality of p forces any prime divisor of $|H\colon \mathrm{Ker}(\pi)|$ to be greater than or equal to p. Thus, $|H\colon \mathrm{Ker}(\pi)|$ lacks prime divisors, hence is equal to 1. But this implies that $H = \mathrm{Ker}(\pi)$, which is normal in G. Contradiction.

5. Let G be a finite group and $\pi\colon G \to \mathrm{GL}(V)$ a finite-dimensional complex representation. Let χ be the character of π. Show that the characters of the representations on $V \otimes V$, $\mathrm{Sym}^2(V)$ and $\bigwedge^2(V)$ are $\chi(g)^2$, $(\chi(g)^2 + \chi(g^2))/2$ and $(\chi(g)^2 - \chi(g^2))/2$. (Hint: Express $\chi(g)^2$, $(\chi(g)^2 + \chi(g^2))/2$ and $(\chi(g)^2 - \chi(g^2))/2$ in terms of the eigenvalues of $\pi(g)$.)

Solution: Since $\pi(g)$ is a unitary matrix, we can choose (by the Spectral Theorem) a basis $\{e_1, \dots, e_n\}$ of V consisting of eigenvectors for $\pi(g)$, say

$$\pi(g)(e_i) = \lambda_i e_i.$$

By definition, $\chi(g) = \mathrm{tr}(\pi(g)) = \sum_{i=1}^n \lambda_i$.

Note that $\{e_i \otimes e_j \colon i, j = 1, \dots, n\}$ is a basis for $V \otimes V$. Note also that

$$\begin{aligned}\pi_{V\otimes V}(g)(e_i \otimes e_j) &= \pi(g)(e_i) \otimes \pi(g)(e_j)\\ &= \lambda_i e_i \otimes \lambda_j e_j\\ &= \lambda_i \lambda_j (e_i \otimes e_j).\end{aligned}$$

Therefore,

$$\chi_{V\otimes V}(g) = \mathrm{tr}(\pi_{V\otimes V}(g)) = \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j = \sum_{i=1}^n \lambda_i^2 + 2\sum_{i\neq j} \lambda_i \lambda_j = \left(\sum_{i=1}^n \lambda_i\right)^2 = \chi(g)^2$$

Note that $\{e_i \otimes e_j + e_j \otimes e_i \colon i \le j\}$ is a basis for $\mathrm{Sym}^2(V)$. Note also that $\pi_{\mathrm{Sym}^2(V)} = \pi_{V\otimes V}|_{\mathrm{Sym}^2(V)}$, so that

$$\begin{aligned}\pi_{\mathrm{Sym}^2(V)}(g)(e_i \otimes e_j + e_j \otimes e_i) &= \pi_{V\otimes V}(g)(e_i \otimes e_j + e_j \otimes e_i)\\ &= \lambda_i\lambda_j(e_i \otimes e_j) + \lambda_j \lambda_i (e_j \otimes e_i)\\ &= \lambda_i \lambda_j (e_i \otimes e_j + e_j \otimes e_i).\end{aligned}$$

Therefore,

$$\begin{aligned}\chi_{\mathrm{Sym}^2(V)}(g) = \mathrm{tr}(\pi_{\mathrm{Sym}^2(V)}(g)) = \sum_{i\le j} \lambda_i\lambda_j &= \sum_{i=1}^n \lambda_i^2 + \sum_{i<j} \lambda_i \lambda_j\\ &= \frac{1}{2}\left[\left(\sum_{i=1}^n \lambda_i\right)^2 + \sum_{i=1}^n \lambda_i^2\right]\\ &= \frac{1}{2}\left[\chi(g)^2 + \chi(g^2)\right],\end{aligned}$$

where we have used the fact that $\chi(g^2) = \mathrm{tr}(\pi(g^2)) = \mathrm{tr}(\pi(g)^2) = \sum \lambda_i^2$.

Note that $\{e_i \otimes e_j - e_j \otimes e_i \colon i < j\}$ is a basis for $\bigwedge^2(V)$. Note also that $\pi_{\bigwedge^2(V)} = \pi_{V\otimes V}|_{\bigwedge^2(V)}$. Thus, by a similar calculation as above, we find

$$\pi_{\bigwedge^2(V)}(g)(e_i \otimes e_j - e_j \otimes e_j) = \lambda_i\lambda_j(e_i \otimes e_j - e_j \otimes e_i),$$

so that

$$\chi_{\bigwedge^2(V)}(g) = \mathrm{tr}(\pi_{\bigwedge^2(V)}(g)) = \sum_{i<j} \lambda_i \lambda_j = \frac{1}{2}\left[\left(\sum_{i=1}^n \lambda_i\right)^2 - \sum_{i=1}^n \lambda_i^2\right] = \frac{1}{2}\left[\chi(g)^2 - \chi(g^2)\right].$$

6. Let V be a vector space over a field F, and let $B\colon V \times V \to F$ be a symmetric bilinear form. This means that B is bilinear and $B(x, y) = B(y, x)$. Let $q(v) = B(v, v)$.

(a) Show that if the characteristic of F is not 2, then $B(v, w) = \frac{1}{2}(q(v + w) - q(v) - q(w))$. (This obviously implies that if $q = 0$, then $B = 0$.)

> *Solution:* Note that
>
> $$\begin{aligned} q(v + w) = B(v + w, v + w) &= B(v, v) + B(w, v) + B(v, w) + B(w, w) \\ &= q(v) + 2B(v, w) + q(w), \end{aligned}$$
>
> so $q(v + w) - q(v) - q(w) = 2B(v, w)$. Since $\mathrm{char}(F) \neq 2$, we may divide by 2 to conclude.

(b) Give an example where the characteristic of F is 2 and $q = 0$ but $B \neq 0$.

> *Solution:* Take $V = \mathbb{F}_4$. Let $\{v, w\}$ be an $\mathbb{F}_2$-basis for $\mathbb{F}_4$. Note that $\mathbb{F}_4 = \{0, v, w, z\}$, where $z = v + w$. Define $B\colon \mathbb{F}_4 \times \mathbb{F}_4 \to \mathbb{F}_2$ via
>
> $$B(av + bw,\ cv + dw) = ad + bc.$$
>
> It is clear that B is bilinear and symmetric. One can check that $B(0, 0) = B(v, v) = B(w, w) = B(z, z) = 0$, so that $q = 0$. However, $B \neq 0$ since $B(v, w) = 1 \neq 0$.

(c) Show that if the characteristic of F is not 2 or 3 and if $B(u, v, w)$ is a symmetric trilinear form, and if $r(v) = B(v, v, v)$, then $r = 0$ implies $B = 0$.

> *Solution:* Note that
>
> $$\begin{aligned} r(v + w) &= B(v + w, v + w, v + w) \\ &= B(v, v, v) + B(v, v, w) + B(v, w, v) + B(v, w, w) \\ &\quad + B(w, v, v) + B(w, v, w) + B(w, w, v) + B(w, w, w) \\ &= r(v) + r(w) + 3B(v, v, w) + 3B(v, w, w), \end{aligned}$$
>
> so that
>
> $$r(v + w) - r(v) - r(w) = 3(B(v, v, w) + B(v, w, w)).$$
>
> Replacing w with $-w$ gives
>
> $$r(v - w) - r(v) + r(w) = 3(-B(v, v, w) + B(v, w, w)).$$
>
> Therefore, $r = 0$ implies both that $B(v, v, w) = -B(v, w, w)$ and $B(v, v, w) = B(v, w, w)$. Hence,
>
> $$B(v, v, w) = 0 \quad \forall v, w \in V.$$
>
> For $w \in V$, define $b_w(v_1, v_2) := B(v_1, v_2, w)$. Then b_w is a symmetric bilinear form with $q_w = 0$. By part (a), we have $b_w = 0$ for all $w \in V$. This means that $B = 0$.

7. Let G be a finite group.

(a) Let $\pi\colon G \to \mathrm{GL}(V)$ be an irreducible complex representation, and let χ be its character. If $g \in G$, show that $|\chi(g)| = \dim(V)$ if and only if there is a scalar $c \in \mathbb{C}$ such that $\pi(g)v = cv$ for all $v \in V$.

Solution:

($\Longleftarrow$) Suppose there exists $c \in \mathbb{C}$ such that $\pi(g)v = cv$ for all $v \in V$. Then every $g \in G$ has $\pi(g) = c \cdot \mathrm{Id}_V$. Since $\pi(g)$ is a unitary matrix, we have $|\det(\pi(g))| = 1$, so $|c| = 1$. Therefore,

$$|\chi(g)| = |\mathrm{tr}(\pi(g))| = |\mathrm{tr}(c \cdot \mathrm{Id}_V)| = |c \cdot \dim(V)| = \dim(V).$$

($\Longrightarrow$) Suppose $g \in G$ has $|\chi(g)| = \dim(V)$. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $\pi(g)$. Note that

$$|\chi(g)| = |\mathrm{tr}(\pi(g))| = \left|\sum_{i=1}^{n} \lambda_i\right| \leq \sum_{i=1}^{n} |\lambda_i| = n = \dim(V).$$

By hypothesis, equality holds, so that each $\lambda_i = r_i\lambda_1$ for some $r_i > 0$. Since

$$1 = |\lambda_i| = r_i|\lambda_1| = r_i$$

we see that $\lambda_1 = \cdots = \lambda_n$. Since $\pi(g)$ is diagonalizable (Spectral Theorem), it is similar to the matrix $\mathrm{diag}\{\lambda_1, \ldots, \lambda_1\}$. Hence, $\pi(g)v = \lambda_1 v$ for all $v \in V$.

(b) Show that g is in the center $Z(G)$ if and only if $|\chi(g)| = \chi(1)$ for every irreducible character χ of G.

Solution:

($\Longrightarrow$) Suppose $g \in Z(G)$. Let $\pi\colon G \to \mathrm{GL}(V)$ be an irreducible representation of G with character χ. For every $h \in G$, we have

$$\pi(g)\pi(h) = \pi(gh) = \pi(hg) = \pi(g)\pi(h).$$

Thus, Schur's Lemma implies that $\pi(g)$ is a homothety: there exists $c \in \mathbb{C}$ such that $\pi(g)v = cv$ for all $v \in V$. By part (a), it follows that $|\chi(g)| = \dim(V) = \mathrm{tr}(\mathrm{Id}_V) = \chi(1)$.

($\Longleftarrow$) Let $\chi_1, \ldots, \chi_h$ denote the irreducible characters of G. Let $n_1, \ldots, n_h$ denote their respective degrees. By the Orthogonality Relations, every $g \in G$ satisfies

$$\frac{1}{|G|}\sum_{i=1}^{h} |\chi_i(g)|^2 = \frac{1}{|\mathrm{Conj}(g)|},$$

where $\mathrm{Conj}(g)$ denotes the conjugacy class of g.

Suppose $g \in G$ is such that each $|\chi_i(g)| = \chi_i(1) = n_i$. Then

$$\frac{1}{|\mathrm{Conj}(g)|} = \frac{1}{|G|}\sum_{i=1}^{h} n_i^2 = 1.$$

Thus, $|\mathrm{Conj}(g)| = 1$, which means that $g \in Z(G)$.

8. Let V be a vector space of dimension $d \geq 1$ over a field k of arbitrary characteristic. Let V^* denote the dual space.

(a) For any $n \geq 1$, prove that there is a unique bilinear pairing $V^{\otimes n} \times (V^*)^{\otimes n} \to k$ satisfying

$$(v_1 \otimes \cdots \otimes v_n, \ell_1 \otimes \cdots \otimes \ell_n) \mapsto \prod_{i=1}^{n} \ell_i(v_i),$$

and by using bases show that it is a perfect pairing (i.e., identifies $(V^*)^{\otimes n}$ with $(V^{\otimes n})^*$).

Solution: By the universal property of tensor products, the multilinear map

$$\begin{aligned} V \times \cdots \times V \times V^* \times \cdots \times V^* &\to k \\ (v_1, \ldots, v_n, \ell_1, \ldots, \ell_n) &\mapsto \prod \ell_i(v_i) \end{aligned}$$

descends to a linear map

$$\begin{aligned} V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^* &\to k \\ \text{with} \qquad v_1 \otimes \cdots \otimes v_n \otimes \ell_1 \otimes \cdots \otimes \ell_n &\mapsto \prod \ell_i(v_i) \end{aligned}$$

on simple tensors. Again by the universal property, this in turn induces a bilinear map

$$\begin{aligned} \Phi \colon (V \otimes \cdots \otimes V) \times (V^* \otimes \cdots \otimes V^*) &\to k \\ \text{with} \qquad (v_1 \otimes \cdots \otimes v_n, \ell_1 \otimes \cdots \otimes \ell_n) &\mapsto \prod \ell_i(v_i) \end{aligned}$$

on ordered pairs of simple tensors. Since this map is specified on generators, it is unique.

We therefore obtain a linear map

$$\begin{aligned} \varphi \colon (V^*)^{\otimes n} &\to (V^{\otimes n})^* \\ \eta &\mapsto \Phi(\cdot, \eta) \end{aligned}$$

We claim that φ is an isomorphism.

Let $\{e_1, \ldots, e_d\}$ be a basis for V, and let $\{\epsilon^1, \ldots, \epsilon^d\}$ denote the dual basis for V^*. Note that $\{e_{i_1} \otimes \cdots \otimes e_{i_n}\}$ and $\{\epsilon^{j_1} \otimes \cdots \otimes \epsilon^{j_n}\}$ are then bases for $V^{\otimes n}$ and $(V^*)^{\otimes n}$, respectively. We then have

$$\varphi(\epsilon^{j_1} \otimes \cdots \otimes \epsilon^{j_n})(e_{i_1} \otimes \cdots \otimes e_{i_n}) = \Phi(e_{i_1} \otimes \cdots \otimes e_{i_n}, \epsilon^{j_1} \otimes \cdots \otimes \epsilon^{j_n}) = \prod_{k=1}^{n} \epsilon^{j_k}(e_{i_k}) = \prod_{k=1}^{n} \delta_{i_k}^{j_k},$$

where δ_i^j is the Kronecker delta. On the other hand, if $\{\alpha^{j_1 \cdots j_n}\}$ denotes the basis of $(V^{\otimes n})^*$ that is dual to $\{e_{i_1} \otimes \cdots \otimes e_{i_n}\}$, we have

$$\alpha^{j_1 \cdots j_n}(e_{i_1} \otimes \cdots \otimes e_{i_n}) = \prod_{k=1}^{n} \delta_{i_k}^{j_k}.$$

Therefore: $\varphi(\epsilon^{j_1} \otimes \cdots \otimes \epsilon^{j_n}) = \alpha^{j_1 \cdots j_n}$.

Since φ maps a basis of $(V^*)^{\otimes n}$ to a basis of $(V^{\otimes n})^*$, it is an isomorphism.

8. Let V be a vector space of dimension $d \geq 1$ over a field k of arbitrary characteristic. Let V^* denote the dual space.

(b) For any $1 \leq n \leq d$, do similarly with $\bigwedge^n(V)$ and $\bigwedge^n(V^*)$ using the requirement

$$(v_1 \wedge \cdots \wedge v_n, \ell_1 \wedge \cdots \wedge \ell_n) \mapsto \det(\ell_i(v_j)).$$

Solution: For $v = (v_1, \ldots, v_n) \in V^n$, define a map

$$\begin{aligned} f_v \colon V^* \times \cdots \times V^* &\to k \\ (\ell_1, \ldots, \ell_n) &\mapsto \det(\ell_i(v_j)) \end{aligned}$$

Since f_v is multilinear and alternating, it descends to a linear map

$$F_v \colon \bigwedge^n V^* \to k$$

with $F_v(\ell_1 \wedge \cdots \wedge \ell_n) = f_v(\ell_1, \ldots, \ell_n)$ on simple wedge products.

For $\theta \in \bigwedge^n V^*$, define a map

$$\begin{aligned} g^\theta \colon V \times \cdots \times V &\to k \\ g^\theta(v) &= F_v(\theta) \end{aligned}$$

Since g^θ is multilinear and alternating, it descends to a linear map

$$G^\theta \colon \bigwedge^n V \to k$$

with $G^\theta(v_1 \wedge \cdots \wedge v_n) = g^\theta(v_1, \ldots, v_n)$ on simple wedge products.

Finally, define the bilinear map

$$\begin{aligned} H \colon \bigwedge^n V \times \bigwedge^n V^* &\to k \\ H(\eta, \theta) &= G^\theta(\eta). \end{aligned}$$

Note that if $\eta = v_1 \wedge \cdots \wedge v_n$ and $\theta = \ell_1 \wedge \cdots \wedge \ell_n$ are simple wedge products, then

$$H(\eta, \theta) = G^\theta(\eta) = g^\theta(v) = F_v(\theta) = f_v(\ell_1, \ldots, \ell_n) = \det(\ell_i(v_j)),$$

where $v = (v_1, \ldots, v_n)$.

9. Let K/k be a finite extension of fields with $\alpha \in K$ as a primitive element over k. Let $f \in k[x]$ be the minimal polynomial of α over k.

(a) Explain why $K \cong k[x]/(f)$ as k-algebras, and use this to relate the local factor rings of $K \otimes_k F$ to the irreducible factors of f in $F[x]$, with F/k a field extension.

Solution: Let K/k be a finite extension of fields with $\alpha \in K$ as a primitive element. Let $f \in k[x]$ be the minimal polynomial of α over k. Note that the k-algebra homomorphism

$$\begin{aligned} \varphi\colon k[x] &\to k(\alpha) = K \\ p(x) &\mapsto p(\alpha) \end{aligned}$$

is surjective and $\mathrm{Ker}(\varphi) = \{p \in k[x] \colon p(\alpha) = 0\} = (f)$. Thus, we have an induced k-algebra isomorphism $k[x]/(f) \to K$.

From the exact sequence $0 \to (f) \otimes_k F \to k[x] \otimes_k F \to \frac{k[x]}{(f)} \otimes_k F \to 0$, we see that

$$K \otimes_k F \cong \frac{k[x]}{(f)} \otimes_k F \cong \frac{k[x] \otimes_k F}{(f) \otimes_k F} \cong \frac{F[x]}{(f)},$$

where in the last step we used the isomorphisms $k[x] \otimes_k F \cong F[x]$ and $(f) \otimes_k F \cong (f)F$.

Let $f = f_1^{e_1} \cdots f_r^{e_r}$ denote the factorization of f into irreducibles in $F[x]$. By the Chinese Remainder Theorem,

$$K \otimes_k F \cong \frac{F[x]}{(f)} \cong \prod_{i=1}^{r} \frac{F[x]}{(f_i^{e_i})}.$$

Note that each factor $F[x]/(f_i^{e_i})$ in the above product is a local ring.

(b) Assume K/k is Galois with Galois group G. Prove that the natural map $K \otimes_k K \to \prod_{g \in G} K$ defined by $a \otimes b \mapsto (g(a)b)$ is an isomorphism.

Solution: Let $a, b \in K$, writing $a = p(\alpha)$ for some $p \in k[x]$. From the proof of part (a), we have isomorphisms

$$\begin{aligned} K \otimes_k K &\cong \frac{k[x]}{(f)} \otimes_k K \cong \frac{K[x]}{(f)} \\ a \otimes b &\mapsto \overline{p(x)} \otimes b \ \mapsto \ b\,\overline{p(x)}. \end{aligned} \tag{1}$$

Note that $f(x) = \prod_{g \in G}(x - g(\alpha))$ in $K[x]$. Therefore, by the Chinese Remainder Theorem,

$$\begin{aligned} \frac{K[x]}{(f)} &\cong \prod_{g \in G} \frac{K[x]}{(x - g(\alpha))} \cong \prod_{g \in G} K \\ r(x) &\mapsto (r(x) \bmod (x - g(\alpha)) \mapsto (r(g(\alpha))). \end{aligned} \tag{2}$$

Composing the isomorphisms (1) and (2), and noting that $r(g(\alpha)) = g(r(\alpha))$, we have

$$\begin{aligned} K \otimes_k K &\cong \prod_{g \in G} K \\ a \otimes b &\mapsto (g(a)b). \end{aligned}$$

10. Let G be a finite abelian group, $\omega\colon G \times G \to \mathbb{R}/\mathbb{Z}$ a bilinear mapping such that

(i) $\omega(g,g) = 0$ for all $g \in G$;

(ii) $\omega(x,g) = 0$ for all $g \in G$ if and only if x is the identity element.

Prove that the order of G is a square. Give an example of G of square order for which no such ω exists.

(Hint: Consider a subgroup A of G which is maximal for the property that $\omega(x,y) = 0$ for all x, y in A. You may use the following fact without proof: any finite abelian group X admits $|X|$ distinct homomorphisms to $\mathbb{R}/\mathbb{Z}$.)

Solution: Consider the map

$$G \to \mathrm{Hom}(G, \mathbb{R}/\mathbb{Z})$$
$$x \mapsto \omega(x, -)$$

Property (ii) says exactly that this map is injective. Since $|G| = |\mathrm{Hom}(G, \mathbb{R}/\mathbb{Z})|$ (by the Hint), it follows that this map is surjective.

Consider the inclusion $0 \to A \hookrightarrow G$. Since $\mathbb{R}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the Hom sequence $\mathrm{Hom}(G, \mathbb{R}/\mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z}) \to 0$ is exact. That is, the restriction map

$$\mathrm{Hom}(G, \mathbb{R}/\mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z})$$
$$\sigma \mapsto \sigma|_A$$

is surjective.

Combining these two observations, we see that the composed map

$$\varphi\colon G \to \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z})$$
$$x \mapsto \omega(x, -)|_A$$

is surjective. We claim that $A = \mathrm{Ker}(\varphi)$.

By definition of A, we clearly have $A \subset \mathrm{Ker}(\varphi)$. Conversely, suppose $x \in \mathrm{Ker}(\varphi)$, so that $\omega(x,a) = 0$ for all $a \in A$. By (i), we have

$$0 = \omega(x+a, x+a) = \omega(x,x) + \omega(x,a) + \omega(a,x) + \omega(a,a) = \omega(a,x)$$

so that $\omega(a,x) = 0$ for all $a \in A$. Suppose for the sake of contradiction that $x \notin A$. Consider the group $A' = \langle A, x \rangle$ generated by A and x. If $a + mx, a' + nx \in A'$, then

$$\omega(a + mx, a + nx) = \omega(a,a) + m\,\omega(x,a) + n\,\omega(a,x) + mn\,\omega(x,x) = 0.$$

Thus, every $y_1, y_2 \in A'$ has $\omega(y_1, y_2) = 0$, which contradicts the maximality of A.

Therefore, we have an isomorphism

$$G/A \cong \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z}),$$

which implies that $|G| = |A|^2$.

Example: Let $G = \mathbb{Z}/4\mathbb{Z}$. If $\omega\colon G \times G \to \mathbb{R}/\mathbb{Z}$ is a bilinear map satisfying (i), then $\omega(1,1) = 0$. But this implies that $\omega(1,3) = \omega(1,2) = \omega(1,1) = \omega(1,0) = 0$, which means that (ii) cannot hold.