445 Assignment 1: Due September 24, 2015, in class

Exercise 1. *Let F be a field. Show that every finite group embeds into $\mathrm{GL}_n(F)$ for some $n \geq 1$.*

Exercise 2. *Let G denote the group consisting of bijective maps f from $\mathbb{Z}$ to itself such that f fixes all but finitely many integers. Show that there does not exist a field F and an $n \geq 1$ such that G embeds in $\mathrm{GL}_n(F)$.*

Exercise 3. *Show that a group homomorphism $\phi : G \to \mathrm{GL}_n(F)$ extends to a ring homomorphism $\psi : F[G] \to \mathrm{M}_n(F)$ and that if V is the set of $n \times 1$ column vectors with entries in F then V is a left $F[G]$-module.*

Exercise 4. *Show that being left artinian is equivalent to every non-empty set of left ideals having a minimal element (not necessarily unique) with respect to inclusion.*

Exercise 5. *Prove that a finite division ring is a field using the following steps. Let D be a finite division ring.*

1 *Show that the centre Z of D is a field and has size q for some prime power q. Show that D has size q^n for some $n \geq 1$.*

2 *Let $G = D^*$ be the multiplicative group of D. Then $|G| = q^n - 1$. Use the class equation to show that*

$$q^n - 1 = |Z| + \sum_g |C_g| = q - 1 + \sum_g (q^n - 1)/|C(g)|,$$

where the sums runs over a complete set of non-central conjugacy class representatives and C_g denotes the conjugacy class of g and $|C(g)|$ denotes the centralizer of g in G.

3 *Show that if $g \in D^*$ then the centralizer of g in D is a division ring E that properly contains Z. Conclude that $|C(g)| = q^m - 1$ for some m.*

4 *Show that $q^m - 1$ divides $q^n - 1$ if and only if m divides n. Conclude that $|C(g)| = q^d - 1$ for some d dividing n and $d > 1$.*

5 *Rewrite the class equation as*

$$q^n - 1 = (q - 1) + \sum_{j=1}^{r} (q^n - 1)/(q^{d_j} - 1),$$

where r is the number of non-central conjugacy class representatives $d_1, \ldots, d_r > 1$ are divisors of n.

6 *Remember! Our goal is to show that D is a field, so we want to show $D = Z$ and so $n = 1$. Let $P(x) = \prod(x - \zeta)$, where ζ runs over all primitive n-th roots of unity. You can use the following fact: $P(x)$ is a monic polynomial with integer coefficients. (We'll show this later on when we talk about characters, but if you know a bit of Galois theory, you can convince yourself that the coefficients of $P(x)$ are fixed by the Galois group of $\mathbb{Q}(\exp(2\pi i/n))$ over $\mathbb{Q}$ and so the coefficients are rational; also ζ is an algebraic integer since it satisfies $\zeta^n - 1 = 0$—since the algebraic integers form a ring we see the coefficients are rational algebraic integers and hence integers. If you don't understand this, don't worry about it.) Show that $(x^n - 1) = P(x)Q(x)$ where $Q(x)$ is a monic integer polynomial and $x^d - 1$ divides $Q(x)$ in $\mathbb{Z}[x]$ for every divisor d of n with $d < n$.*

7 *Now show from step 5 that $P(q)$ divides $q - 1$.*

8 *Now we're ready to finish. Show that if $n > 1$ then $|P(q)| > q - 1$ and conclude that $n = 1$ and $D = Z$.*

Exercise 6. *Let R be a finite ring and suppose that for each $x \in R$ there is some $n = n(x) > 1$ such that $x^n = x$. Show using the Artin-Wedderburn theorem and Wedderburn's theorem on finite division rings that R is commutative.*

Exercise 7. *Let F be an algebraically closed field and let R be a finite-dimensional F-algebra and suppose that R has no nonzero nil ideals. Show that R is isomorphic to a finite direct product of matrix rings over F.*

Exercise 8. *Let R be a ring. Show that if S is a subset of R that is closed under multiplication and does not contain zero then there is some prime ideal P of R with $P \cap S = \emptyset$. Conclude by taking $S = \{1\}$ that R always has at least one prime ideal.*

Exercise 9. *Let R be a ring (with identity). Show that the intersection of the prime ideals of R is a nil ideal. (Hint: see if you can use the preceding exercise.)*

Exercise 10. *Let R be the $\mathbb{C}$-algebra with generators x and y and relations $xy = 2yx$. (You can think of R as being a polynomial ring in 2-variables x and y but where the variables skew-commute. Show that R is primitive and xR is a two-sided proper ideal of R. Conclude that R is prime, primitive, but not simple. Let $S = \mathbb{C}[x]$. Show that S is prime but not primitive. (Hint: primitivity of R is tricky. Here's how one can do it. First show that every nonzero ideal of R contains an element of the form $(xy)^a$ with $a \geq 1$. Now let $I = R(xy - 1)$. Show that I is a proper left ideal. Use Zorn's lemma to show that there is a maximal left ideal L containing I. Then $M := R/L$ is a simple left R-module. Show that it must be faithful.)*