Assignment 4: Due April 2, 2019

Let's do some basic things with division rings. Recall that a division ring is an associative ring in which every nonzero element has an inverse. Some theorems that you might not know, but that are useful are the Artin-Wedderburn theorem. We'll use a very special case that you might have seen if you took representation theory: if F is an algebraically closed field and A is a finite-dimensional simple F-algebra then $A \cong M_n(F)$ for some n.

1 Let D be a division ring. Show that the centre $Z = \{x \in D \colon zx = xz\}$ is a field.

2 Let D be a division ring and let Z be its centre. We say that D is finite-dimensional if $[D : Z] < \infty$; i.e., D is finite-dimensional as a Z-vector space. Show that if D is a finite-dimensional division ring and F is a field extension of Z then $B := D \otimes_Z F$ is a simple F-algebra whose centre is $F \cong Z \otimes_Z F$ and $\dim_F(B) = \dim_Z(D)$. (Hint: to show that it is simple, first do the part about the centre. Now Let I be a nonzero ideal and pick nonzero $x = \sum_{i=1}^{s} a_i \otimes \lambda_i \in I$ with s minimal, where the $a_i \in D$ and $\lambda_i \in F$. First show by minimality of s that you may assume that the a_i are linearly independent over Z and the λ_i are linearly independent over Z and that $a_1 = 1$ and $\lambda_1 = 1$. Next show that if $s = 1$ then $x = 1$ under these assumptions, so if you can show that $s = 1$, you're done. So now assume $s > 1$. Show that if $x(b \otimes \gamma) - (b \otimes \gamma)x$ has shorter length, so show that x is central and use your description of the centre to finish things off.)

3 Use the Artin-Wedderburn theorem to show that if D is a finite-dimensional division ring then $[D : Z]$ is a perfect square. (Hint: Look at $D \otimes_Z \bar{Z}$, where $\bar{Z}$ is the algebraic closure of Z.)

4 Let K be a field and assume that there is $\omega \in K$ with ω an n-th root of unity. Let $a, b \in K \setminus \{0\}$. Define a ring $R = K\{x, y\}/(x^n - a, y^n - b, xy - \omega yx)$. Show that R is an n^2-dimensional K-algebra. (Hint: put a dlex order on monomials by declaring that $x > y$ and show that the relations given yield a Gröbner-Shirshov basis and that the monomials that do not have initial terms as subwords are those of the form $y^i x^j$ with $i, j < n$. Show also that R is simple.

5 Let K be a field, let $n = 2$, $\omega = -1$, $a = b = -1$. Show that the R from the preceding example is a division ring if zero cannot be written as a non-trivial sum of at most four squares in K (e.g., fields such at $\mathbb{Q}$ and $\mathbb{R}$) and show that it is isomorphic to $M_2(K)$ if 0 can be written as a sum of at most four nonzero squares (e.g., fields like $\mathbb{Q}(i)$ and $\mathbb{C}$). In the former case, we call R the division ring of quaternions over K. (Hint: Show that $1, i := x$, $j := y$, and $k := xy$ is a K-basis for R now show that if $u := a + bi + cj + dk$ is a zero divisor then so is uu^*, where $u^* = a - bi - cj - dk$ and that $uu^* = u^*u = a^2 + b^2 + c^2 + d^2$.)

6 Let $H = \{a + bi + cj + dk \colon 2a, 2b, 2c, 2d \in \mathbb{Z}, 2a \equiv 2b \equiv 2c \equiv 2d \pmod 2\}$. Show that H is a subring of the division ring of quaternions over $\mathbb{Q}$ and that if $u \in H$ then $N(u) := uu^* = u^*u$ is a positive integer and is nonzero whenever u is nonzero, and that $N(uv) = N(u)N(v)$.

7 Show that H has a left-division algorithm given as follows: If $a, b \in H$ with $b \neq 0$ then there exist $q, r \in H$ such that $a = qb + r$ with $N(r) < N(b)$. (Hint: this is a bit tricky, but it is much easier when b is a positive integer, so do this case first. Now let $n = bb^* > 0$ and do the case you've just done to get $ab^* = qn + r$ with $N(r) < N(n) = n^2$. Now here's the fun part: $r = ab^* - qn = ab^* - qbb^* = (a - qb)b^*$. Let $r' = a - qb$. Show that $N(r') < N(b)$!)

8 Use the preceding result to show that every left ideal of H can be generated by a single element as a left ideal.

9 Show that if $a, b \in H$ are nonzero and are such that $N(a) = N(b)$ and $a = ub$ with $u \in H$, then u is a unit of H.

10 Show that every positive integer can be written as a sum of 4 squares (including 0 as a square). (Hint: using questions 5 and 6 that it is enough to prove that every prime number is a sum of four squares. Let $p \geq 3$ be prime (I assume you can write $p = 2$ as a sum of four squares) and let R_p be the algebra produced in question 4 with $K = \mathbb{F}_p$, $n = 2$, $\omega = -1$, $a = b = -1$. Show R_p is not commutative if $p > 2$ and use Wedderburn's theorem to show that R_p cannot be a division ring. OK, so now let I denote the two-sided ideal of H given by $\{a + bi + cj + dk \colon 2a, 2b, 2c, 2d \in \mathbb{Z}, 2a \equiv 2b \equiv 2c \equiv 2d \pmod 2, p|2a, p|2b, p|2c, p|2d\}$. Show that I is indeed an ideal and that H/I is isomorphic to R_p. What next? Since R_p is not a division ring it has a nonzero proper left ideal J. Then by correspondence, there is a proper left ideal J' of H that properly contains I. Show that every element $u \in J'$ must have the property that $N(u)$ is a multiple of p since otherwise we could generate the unit ideal. By the preceding question, J' can be generated by a single element $a := A + Bi + Cj + Dk \in J' \setminus I$ with $N(a)$ a multiple of p. Since $p \in J'$ we have $p = ba$ for some $b \in H$. Then $N(p) = N(b)N(a)$. Now $N(p) = p^2$ and $N(b)$ and $N(a)$ are integers and $N(a)$ is a multiple of p, so $N(a) \in \{p, p^2\}$. Show using question 9 that if $N(a) = p^2$ then $p = ba$ with b a unit of H and this cannot occur since J' properly contains I. Conclude that $N(a) = p$. What does this mean? It means $p = A^2 + B^2 + C^2 + D^2$. There's just one problem: A, B, C, D are not necessarily integers—they are only half integers and $2A, 2B, 2C, 2D$ have the same parity. But we're close. But let $A' = 2A$, $B' = 2B$, $C' = 2C$, $D' = 2D$, so now we have integers and we have $4p = (A')^2 + (B')^2 + (C')^2 + (D')^2$ and A', B', C', D' have the same parity. OK, now let $X = (A' - B')/2$, $Y = (A' + B')/2$, $Z = (C' - D')/2$, $W = (C' + D')/2$. What happens?)