VIGRE Algebra QR Review, December 9, 2002

Summary of Session

1. Let F be the splitting field over the rational numbers $\mathbb{Q}$ of the polynomial $x^4 - 3$.

(a) Explain why the Galois group of F over $\mathbb{Q}$ may be thought of as a subgroup G of the permutations of the set $\{\sqrt[4]{3},\ -\sqrt[4]{3},\ i\sqrt[4]{3},\ -i\sqrt[4]{3}\}$ where $\sqrt[4]{3}$ is the positive real fourth root of 3, and $i^2 = -1$. Note that $i \in F$.

(b) Show that $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$, and determine $[F : \mathbb{Q}]$.

(c) Prove that G is generated by the transposition $\tau = (i\sqrt[4]{3}, -i\sqrt[4]{3})$ and the 4-cycle σ corresponding to the automorphism of F that fixes i and $-i$ and sends $\sqrt[4]{3}$ to $i\sqrt[4]{3}$. Complete the description of σ as a 4-cycle $(\sqrt[4]{3},\ i\sqrt[4]{3},\ c,\ d)$, i.e., what are the explicit values of c and d? Conclude that $G \cong$ the group of symmetries of a square.

(d) How many subgroups of G have order 2, and how many cyclic subgroups have order 4? You may assume that G has two subgroups of order 4 that are not cyclic. How many subgroups does G have in all? How many fields K are there with $\mathbb{Q} \subseteq K \subseteq F$?

(e) Assume that G has a unique normal subgroup of order 2. How many of the field extensions of $\mathbb{Q}$ in F that have degree 4 are normal? How many of the field extensions of $\mathbb{Q}$ in F that have degree 2 are normal? Explain.

Solution. (a) Since the Galois group stabilizes the equation, it must permute the roots. Since the roots generate the splitting field, any automorphism of the splitting field is uniquely determined by its action on these roots.

(b) If there were a linear or quadratic factor the constant term would be a fourth root of 3 or a square root of 3, and in either case $\sqrt{3}$ would be in $\mathbb{Q}(i)$, so that $Q(\sqrt{3}, i)$ would have degree 2 over $\mathbb{Q}$, and it would follow that $i \in \mathbb{Q}(\sqrt{3})$, a contradiction. It follows that $F = \mathbb{Q}(i)(\sqrt[4]{3})$ has degree 4 over $\mathbb{Q}(i)$ and, hence, degree 8 over $\mathbb{Q}$.

(c) Since $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$ there is an automorphism σ of F that sends $\sqrt[4]{3}$ to $i\sqrt[4]{3}$ while fixing $\mathbb{Q}(i)$, i.e., fixing i. Then $\sigma(i\sqrt[4]{3}) = \sigma(i)\sigma(\sqrt[4]{3}) = i(i\sqrt[4]{3}) = -\sqrt[4]{3}$, and $\sigma(-\sqrt[4]{3}) - -\sigma(\sqrt[4]{3}) = -i\sqrt[4]{3}$, and it follows that σ corresponds to the 4-cycle $(\sqrt[4]{3},\ i\sqrt[4]{3},\ -\sqrt[4]{3},\ -i\sqrt[4]{3})$, i.e., $c = -\sqrt[4]{3}$, $d = -i\sqrt[4]{3}$. Then σ^2 corresponds to $(\sqrt[4]{3},\ -\sqrt[4]{3})\,(i\sqrt[4]{3},\ -i\sqrt[4]{3})$. Complex conjugation clearly gives an element of F, and this is $\tau = (i\sqrt[4]{3},\ -i\sqrt[4]{3})$. Since τ is not a power of σ (it has order two, and would have to be $\sigma^2 = (\sqrt[4]{3},\ -\sqrt[4]{3})\,(i\sqrt[4]{3},\ -i\sqrt[4]{3})$), τ and σ must generate G. Since G has order 8 and is embedded in S_4, it is a 2-Sylow subgroup of S_4 as is the group of symmetries of a square.

(d) The group of symmetries of the square has two elements of order 4 occurring in its unique cyclic subgroup of order 4. There is one element of order 2 in that cyclic subgroup, and it is in the center, and there are four other elements of order 2. Thus, there are 5 subgroups of order 2, and the total number of subgroups is $1 + 5 + 2 + 1 + 1 = 10$. Hence, there are also ten intermediate fields, the fixed fields of these various subgroups.

(e) A subgroup of order 2 is normal if and only if its generator is in the center, i.e., if and only if there is only one element in the conjugacy class of its generator. Thus there is only one normal subgroup of order two, and so only one normal intermediate field extension of degree 4. On the other hand, any subgroup of index 2 is normal, and so there are three normal field extensions of degree 2. (It is not required to specify these, but the normal field extension of degree 4 is $\mathbb{Q}(i, \sqrt{3})$ while the three normal quadratic extensions are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(i, \sqrt{-3}$. The four non-normal extensions of degree 4 are obtained by adjoining just one of the roots of $x^4 - 3$ to $\mathbb{Q}$.)

2. Let S be the ring of Gaussian integers, i.e., $\mathbb{Z}[i] \subseteq \mathbb{C}$, where $\mathbb{Z}$ is the integers and i is a square root of -1. You may assume that this ring is a principal ideal domain.

Let M be the rank 3 free module S^3, and let N be the submodule of M spanned over S by the elements $(1, i, 4)$ and $(2, 3 + 2i, 14)$. Explicitly express M/N as a direct sum of cyclic S-modules.

Solution. One may perform elementary row and column operations on the matrix over S formed from the given rows without affecting the result of killing the row space. (One may, of course, use columns instead.) Subtracting the first row from the second gives rows $(1, i, 4)$ and $(0, 3, -5)$. Subtracting i times the first column from the second and adding 5 times the first column to the last produces rows $(1, 0, 0)$ and $(0, 3, 6)$. Subtracting twice the second column from the last produces $(1, 0, 0)$ and $(0, 3, 0)$. The quotient is now clearly $(S/3S) \oplus_S S$.

3. (a) Show that if every element of a group G has finite odd order, then for every element $g \in G$ there is an element $x \in G$ such that $x^2 = g$.

(b) Show that if G is a finite group and for every element $g \in G$ there is an element $x \in G$ such that $x^2 = g$, then G has odd order.

Solution. (a) If g has order $2n - 1$, so that $g^{2n-1} = e$, then $g^{2n} = g$, so that $x = g^n$ has the required property.

(b) Since the order of G is even it contains elements of order 2. Let $g \in G$ be such that its order is a power of 2 and as large as possible, say 2^m. Let $x^2 = g$. Then $x^{2^{m+1}} = (x^2)^{2^m} = e$, so that the order of x divides 2^{m+1}. But it does not divide 2^m, or else $x^{2^m} = e$, and $x^{2^m} = (x^2)^{2^{m-1}} = g^{2^{m-1}} \neq e$. Thus, x has order 2^{m+1}, a contradiction.

4. Let K be a field, let n be a positive integer, and let V be a vector space over K of dimension n. Suppose that $T : V \to V$ is K-linear. Is it true that T is nilpotent if and only if for all integers k, $1 \leq k \leq n$, the trace of $\bigwedge^k T : \bigwedge^k V \to \bigwedge^k V$ is zero? Prove your answer.

Solution. One method is to show that the eigenvalues of $\bigwedge^k T$ in an algebraic closure of K are the products of the eigenvalues of T taken k at a time. This is easily checked for diagonal matrices, and, hence, for matrices that are diagonalizable. The result for a matrix of indeterminates follows, because it has distinct eigenvalues and is therefore diagonalizable. The general case follows from the case of indeterminates. (Alternatively, one can work over an algebraic closure, take a matrix for T which is upper triangular, and show that $\bigwedge^k T$ has a matrix which is upper triangular and whose diagonal entries are the products of the eigenvalues of T taken k at a time.) The trace condition implies that the sum of the products of the eigenvalues taken k at a time is 0 for $1 \le k \le n$, which implies that all coefficients of the characteristic polynomial except the leading coefficient are 0. The characteristic polynomial is therefore x^n, and so the matrix is nilpotent.

5. Let A be a $n \times n$ matrix over the complex numbers $\mathbb{C}$ that satisfies the equations $A^4 = A$ and $A^3 = 3A^2 - 2A$. What are the possibilities for the minimal polynomial of A? How many possibilities are there for the similarity class of A? Describe the possible Jordan forms.

Solution. A satisfies $x^4 - x = x(x-1)(x^2+x+1)$ and $x^3 - 3x^2 + 2x = x(x-1)(x-2)$. This is equivalent to the statement that A satisfies the GCD, which is $x(x-1)$. Thus, the minimal polynomial of A has distinct roots, so that A is diagonalizable, each of which is 0 or 1. Since the order of the eigenvalues on the diagonal does not affect the similarity class, there are n possibilities: one may think of this as the number of 1 's among the eigenvalues, and is the same as the rank of the matrix. A typical Jordan form consists of a diagonal matrix with r occurrences of 1 and $n - r$ of 0 on the diagonal.

6. Let K be a field and let $R = K[x]$ be the polynomial ring in one variable over K. Let M be a finitely generated torsion module over $K[x]$.

(a) Explain why M must be finite dimensional as a K-vector space.

(b) Prove that M is the cokernel of an $r \times r$ matrix A with entries in $K[x]$ for some r. (The cokernel is the quotient of $K[x]^{\oplus r}$ by the column space of the matrix.)

(c) Prove that if $M \cong R/(f_1) \oplus \cdots \oplus R/(f_k)$ is any way of writing M as a direct sum of cyclic modules, then the product of the f_j is the same, up to multiplication by a scalar in $K - \{0\}$, as $\det A$, where A is chosen as in part (b). Conclude that $\det A$ is independent, up to multiplication by a nonzero scalar, of the choice of A. (Note that both k and the size of A may vary even though M is fixed.)

Solution. M is a direct sum of finitely many cyclic modules $K[x]/(g_j)$, $1 \le j \le r$, and if M is torsion the g_j are nonzero. Then $K[x]/(g_j)$ is a K-vector space of dimension $d_j = \deg g_j$, so that the K-vector space dimension of M is the same as the sum of the d_j, and is finite. Moreover, M is the cokernel of the $r \times r$ diagonal matrix whose entries are the g_j. The determinant is the product of the g_j. This takes care of parts (a) and (b). To handle the third part, it suffices to show that if two square matrices (possibly of different sizes) have the same cokernel, then their determinants are the same up to a nonzero scalar multiple. We can perform elementary row and column operations on each of the two matrices (adding a multiple of a row or column to another, which does not change the determinant, permuting rows or columns, which only changes the sign, and multiplying a row or column by a nonzero scalar, which changes the determinant by multiplying it by that same scalar) without affecting whether the result is true. The matrix can be brought by such operations to diagonal form, where the diagonal elements are monic polynomials such that each divides all polynomials that follow it, and this form is unique except that the larger matrix may have more diagonal entries equal to 1 after these operations are performed. Thus, once one performs the elementary operations, the two matrices have the same determinant, and so their original determinants were the same up to a nonzero scalar multiplier.

7. Let $f(x)$ be a nonconstant polynomial over the rational numbers $\mathbb{Q}$ with splitting field F, and let G be the Galois group of F over $\mathbb{Q}$. Let S_n denote the symmetric group on n elements and A_n the alternating group on n elements. Suppose that $G_3 \subseteq G_2 \subseteq G_1 = G$ are subgroups of G such that G_{i+1} is normal in G_i for $i = 1, 2$. Suppose that $G_3 = A_4 \times S_4$, that $|G_2|/|G_3| = 11^7$, and that $|G_1|/|G_2| = 68$. Does this information determine whether f is solvable by radicals? If so, is it solvable by radicals? Explain your answer carefully, making explicit the statements of any major theorems that you use.

Solution. Since every group of order smaller than 60 is solvable, both A_4 and S_4 are solvable, and, hence, so is their product. G_2/G_3 is a p-group with $p = 11$, and therefore it is nilpotent, and, hence, solvable. G_1/G_2 has order $68 = 4 \cdot 17$. The number of subgroups of order 17 divides 4 and is $\equiv 1 \bmod 17$. Thus, there is a unique subgroup of order 17, which must be normal. The quotient has order 4 and so is abelian and, therefore, solvable. Thus, G_1/G_2 is solvable, since an extension of a solvable group by a solvable group is solvable, and for the same reason we have first that G_2 is solvable and then that G is solvable. This implies that f is solvable by radicals: this is equivalent to the solvability of the Galois group in characteristic 0.

8. Determine the behavior of the rank and signature of the matrix $\begin{pmatrix} 1 & 4 & 9 \\ 4 & 17 & 38 \\ 9 & 38 & r \end{pmatrix}$ as r varies in the real numbers. For which values of r is it positive definite? For which values of r is it non-degenerate?

Solution. We preserve the cogredience class by performing elementary operations, but for each row operation we perform we also perform the corresponding column operation, and conversely. Thus, we subtract 4 times the first row from the second and 4 times the first column from the second. We then subtract 9 times the first row from the third and 9 times the first column from the third. Finally, we subtract twice the second row from the third and then twice the second column from the third:

$$\begin{pmatrix} 1 & 4 & 9 \\ 4 & 17 & 38 \\ 9 & 38 & r \end{pmatrix} \to \begin{pmatrix} 1 & 4 & 9 \\ 0 & 1 & 2 \\ 9 & 38 & r \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 9 \\ 0 & 1 & 2 \\ 9 & 2 & r \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 9 \\ 0 & 1 & 2 \\ 0 & 2 & r-81 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & r-81 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & r-85 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & r-85 \end{pmatrix}.$$

Thus, the rank is three unless $r = 85$, when the rank is two. The form is non-degenerate precisely when $r \neq 85$ and positive definite precisely if $r > 85$. If $r > 85$ the rank is 3 and the signature is $(3, 0, 0)$ (or $3 - 0 =$). If $r = 85$, the rank is 2 and the signature is $(2, 0, 1)$, or $2 - 0 = 2$. If $r < 85$ the rank is 3 and the signature is $(2, 1, 0)$ (or $2 - 1 = 1$).

9. Given an integer d which is not a square, denote by $\mathbb{Z}[\sqrt{d}]$ the ring $\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

(a) Prove that if $d < 0$, then the group of units in $\mathbb{Z}[\sqrt{d}]$ is finite.

(b) Show that the group of units in $\mathbb{Z}[\sqrt{2}]$ is infinite.

Solution. The field $\mathbb{Q}(\sqrt{d})$ has an automorphism that fixes $\mathbb{Q}$ and sends $\sqrt{d}$ to $-\sqrt{d}$: if a, $b \in \mathbb{Q}$, its value on $a + b\sqrt{d}$ is $a - b\sqrt{d}$. This automorphism maps $\mathbb{Z}[\sqrt{d}]$ bijectively to itself, and so gives an automorphism of the ring. If $a + b\sqrt{d}$ is a unit, so its image under any automorphism. This implies that $a - b\sqrt{d}$ is also a unit and, hence, so is their product, $a^2 - b^2 d = h$. But if an integer h is a unit in $\mathbb{Z}[\sqrt{d}]$, then for suitable integers u, v we have that $h(u + v\sqrt{d}) = 1$, which yields that $hu = 1$ while $hv = 0$. This implies that $v = 0$, and $h = \pm 1$. From this we conclude that $a + b\sqrt{d}$ is a unit if and only if $a^2 - b^2 d = \pm 1$. If $d = -k$ is a negative integer we must have $a^2 + kb^2 = 1$, and this cannot hold unless unless $b = 0$, $a = \pm 1$ or $a = 0$, $k = 1$, and $b = \pm 1$. This shows that there are at most 4 units. When $d = 2$, the units correspond to solutions of $a^2 - 2b^2 = \pm 1$. By inspection, $a = 3$, $b = 2$ gives the unit $3 + 2\sqrt{2}$. Since this element is > 1, its powers are all distinct, and there are infinitely many units in the ring.

10. Let $p \geq 3$ be a prime integer, and let G be the group of 3×3 upper triangular matrices over $\mathbb{Z}_p$ such that all diagonal entries are equal to 1.

(a) What is the order of G? On the basis of your answer, can you predict whether the center of G is trivial?

(b) Determine the possible orders of the elements of G.

(c) Is G abelian?

(d) If the center of G is non-trivial, give explicitly a non-trivial element in the center.

(e) Is G solvable? Is G nilpotent? Explain your answers.

Solution. (a) Each matrix has all but three entries specified, and there are p possibilities for each of those entries. Thus, the group has p^3 elements, and this is the order. Since the group is a finite p-group, it is nilpotent, and therefore the center is non-trivial.

(b) Any element other than identity can be written as $1 + N$, where N is a nonzero upper triangular matrix with zeros in the diagonal. Thus, N is nilpotent, and since $p \geq 3$ and $N^3 = 0$, we have that $N^p = 0$. Then $(1 + N)^p = 1^p + N^p$ (since 1 and N commute, the binomial theorem applies, and the intermediate terms involve $\binom{p}{i}$ for $1 \leq i \leq p$, and so are 0). Thus $(1 + N)^p = 1$, and every element other than the identity (which has order 1) has order p.

(c) Consider the matrix N with 1 in the $1, 2$ entry and all other entries 0. Let N' be the matrix with 1 in the $2, 1$ entry and all other entries 0. Then NN' has a 1 in the $1, 3$ spot and all other entries 0, while $N'N = 0$. Then $(1 + N)(1 + N') = 1 + N + N' + NN'$ while $(1 + N')(1 + N) = 1 + N + N' + N'N$, and since $NN' \neq N'N$, $1 + N$ and $1 + N'$ do not commute. Thus, G is not abelian.

(d) Consider the matrix V with 1 in the $1, 3$ spot and 0 's elsewhere. Then V kills every upper triangular nilpotent matrix on both the right and on the left, and so for all elements $1 + N$ of the group, $(1 + V)(1 + N) = 1 + V + N = (1 + N)(1 + V)$. Thus, $1 + V$ is in the center.

(e) As already indicated in part (a), G is nilpotent and therefore solvable as well.