VIGRE Algebra QR Review, October 27, 2003

The following problem was discussed. Let G be a finite group of order m and let p be the smallest prime factor of m. Show that a subgroup H of G of index p must be normal.

To do this, let G act on the left cosets of H by left multiplication. This is a transitive action, and so non-trivial on a set of p elements, and therefore gives a homomorphism with non-trivial image Q in S_p, which has order $p! = p(p-1)!$. The order of Q divides m and $p(p-1)!$, whose greatest common divisor is p, since p is the smallest prime factor of m. Since Q cannot be trivial, the homomorphism $G \to S_p$ must have image of order p, and so the kernel N of this homomorphism is a normal subgroup of G of index p. But $N \subseteq H$, since any element of N fixes the coset H and so must be in H. Since N and H both have index p, the index of N in H is 1, i.e., $N = H$, and so H is normal. $\square$

The following problem was also discussed. Let B be a symmetric bilinear form over $\mathbb{R}$ on an n-dimensional vector space with Sylvester invariants or signature (p, q, r): this means that a matrix for B is congruent or cogredient (terminology varies) to a diagonal matrix A with p diagonal entries $= 1$, q diagonal entries $= -1$, and r diagonal entries $= 0$. Choose a basis $u_1, \ldots, u_p, v_1, \ldots, v_q, w_1, \ldots, w_r$ for V with respect to which the matrix of the form has, first, p consecutive diagonal entries $= 1$, then q diagonal entries $= -1$ and, finally, r diagonal entries $= 0$. The value of B on a pair of these basis vectors is the corresponding entry of the matrix, and so is 0 unless the vectors are equal. Every $B(u_i, u_i) = 1$, every $B(v_j, v_j) = -1$, and every $B(w_k, w_k) = 0$.

The first part of the problem requested a proof that the (bilinear) *radical* of B has dimension r. This is defined as the set of vectors w such that $B(w, z) = 0$ for all $z \in V$. Suppose that $w = \sum_i a_i u_i + \sum_j b_j v_j + \sum_k c_k w_k$. Then if w is in the radical we must have $B(w, u_i) = a_i = 0$ for all i, and similarly, $B(w, \boldsymbol{v}_j) = -b_j = 0 = 0$ for all j. Thus, w must be a linear combination of the w_k, and it is clear that any linear combination of the w_k is in the radical. It follows that the radical is the $\mathbb{R}$-span of the w_k, and so has dimension r.

Another problem asked for best possible upper bounds for the invariants p', q', r' of the restriction of V to a subspace $V' \subseteq V$ in terms of p, q, r. Since p can be characterized as the dimension of a maximum subspace of V such that the form restricted to that subspace is positive definite, it is obvious that $p' \leq p$, and this is achieved for any V' containing the span of u_i. Similarly, $q' \leq q$, since q is the dimension of a maximum subspace on which the form is negative definite, this is achieved for $V' \supseteq$ the span of the v_j. The upper bound for r' is rather more subtle: it is $\min\{p, q\} + r = \min\{p + r, q + r\}$.

This number is clearly the maximum dimension of a subspace on which the form vanishes identically: it occurs if we restrict the form to such a subspace. Let $s = \min\{p, q\}$. Then the form vanishes on the space spanned by $u_1 + v_1, \ldots, u_s + v_s, w_1, \ldots, w_r$: note that

$$B(u_i + v_i, u_i + v_i) = B(u_i, u_i) + B(u_i, v_i) + B(v_i, u_i) + B(v_i, v_i) = 1 + 0 + 0 - 1 = 0.$$

We claim that the form cannot vanish identically on any subspace of larger dimension. For suppose that V_0 has dimension larger than $p+r$. Then $\dim V_0 + \dim N > n = p+q+r$, where N is the span of the v_j, and this implies that $V_0 \cap N$ has positive dimension: it will be $\dim V_0 + \dim N - \dim(V_0 + N) \leq \dim V_0 + \dim N - n > 0$. This means that V_0 meets N in a nonzero vector v, and then $B(v,v) < 0$, a contradiction. An exactly similar argument shows that if $\dim V_0 > p+r$ then $V_0 \cap P$ contains a nonzero vector, where P is the span of the u_i, and for such a vector u, $B(u,u) > 0$. Thus, the fact that B vanishes identically on V_0 implies that $\dim V_0$ is $\leq$ both $p+r$ and $q+r$, as required.

A third problem dealt with the Galois group of the extension K of $\mathbb{Q}$ generated by adjunction of the square roots of n distinct positive primes integers, $p_1, \ldots, p_n$. Part of the problem was to show that the Galois group is abelian of order 2^n. Another part was to show that every subfield of K quadratic over $\mathbb{Q}$ is obtained by adjoining the square root of the product of a non-empty subfamily of the p_i.

We shall show by induction on n that the Galois group over the rationals $\mathbb{Q}$ of the field extension K is $\{1,-1\} \times \cdots \times \{1,-1\}$, where there are n copies of the multiplicative group $\{1,-1\} \cong \mathbb{Z}/2\mathbb{Z}$. We shall also show that a basis for K over $\mathbb{Q}$ consists of 1 and the square roots of products of subsets of the primes. After we have established these facts we shall return to the problem of determining all the subfields that are quadratic extensions of $\mathbb{Q}$.

Since the extension is the splitting field of $(x^2 - p_1) \cdots (x^2 - p_n)$ over $\mathbb{Q}$, it is normal, and it is separable, since we are in characteristic 0. Thus, it is Galois. Suppose that we know that $[K : \mathbb{Q}] = 2^n$. Then the Galois group has order 2^n. But each automorphism must permute the roots of $x^2 - p_i = 0$ for all i, and so every automorphism must send p_i to $\epsilon_i p_i$ where $\epsilon_i \in \{1,-1\}$, and is determined by the values of the ϵ_i, since the $\sqrt{p_i}$ generate K over $\mathbb{Q}$. Thus, there are at most 2^n automorphisms, determined by the choices of the ϵ_i. If $[K : \mathbb{Q}] = 2^n$ all of these must occur. Now, if one automorphism sends $\sqrt{p_i}$ to $\epsilon\sqrt{p_i}$ and another to $\epsilon'\sqrt{p_i}$ the composite sends $\sqrt{p_i}$ to $\epsilon\epsilon'\sqrt{p_i}$, and so the Galois group may be identified with n-tuples of elements each of which is in $\{1,-1\}$ under coordinate-wise multiplication.

Thus, it will suffice to show that as we adjoin the square roots of the p_i, at each stage we have a proper extension, which will then be quadratic and have basis $1, \sqrt{p_i}$ over the field constructed by adjoining the square roots of the previous primes. It will then follow that the products of these various square roots together with 1 form a basis by a trivial induction. The case $n = 1$ is obvious, since the equation $x^2 - p_1$ is irreducible over $\mathbb{Q}$.

Thus, we may assume that we know all this for K_0, obtained by adjoining the square roots of $p_1, \ldots, p_{n-1}$, and we need to show that $\sqrt{p_n}$ is not in this field. If it is, it is a rational linear combination of 1 and square roots of products of distinct primes from the various subsets of $p_1, \ldots, p_{n-1}$. If all of the same $\sqrt{p_i}$ for $i \leq n-1$ occur in every nonzero term, then there is only one term and $\sqrt{p_n} = a\sqrt{q}$ where q is the product of a non-empty subset of $p_1, \ldots, p_{n-1}$, while a is rational, so that $p_n/q = a^2$, which is impossible, since the fraction on the left is in lowest terms, and the exponent on p_n is not even. If some $\sqrt{p_i}$ for $i \leq n-1$ does not occur at all, then we get a relation holding with fewer than n primes, contradicting the induction hypothesis. Therefore, there is a $\sqrt{p_i}$ that does not occur in every nonzero term, but that does occur in some nonzero term. Renumbering, we may assume that it is $\sqrt{p_{n-1}}$. Collecting terms, we find that $\sqrt{p_n} = a + b\sqrt{p_{n-1}}$ where a, b are both nonzero and in the field $F = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n_2}})$. By the induction hypothesis there is an automorphism of $F(\sqrt{p_{n-1}})$ that fixes F and sends $\sqrt{p_{n-1}}$ to its negative. This automorphism must send $\sqrt{p_n}$ to $\pm\sqrt{p_n}$, and so we get either the additional equation $\sqrt{p_n} = a - b\sqrt{p_{n-1}}$ or the additional equation $-\sqrt{p_n} = a - b\sqrt{p_{n-1}}$. In the first case we can add the equations to get $2\sqrt{p_n} = 2a$, and so $\sqrt{p_n} = a$, and that means b must have been 0, a contradiction. In the second case we can add the equations to see that $a = 0$, another contradiction.

This shows that $\sqrt{p_n}$ cannot be in the field gotten by adjoining the square roots of the other primes, and we have now established that $[K : \mathbb{Q}] = 2^n$ and that the Galois group is as described earlier.

Finally, we consider the quadratic subfields. By the fundamental theorem of Galois theory, these are in bijective correspondence with the subgroups of index 2 of the Galois group. Each such subgroup is obtained as the kernel of a surjective homomorphism to $\mathbb{Z}/2\mathbb{Z}$ in a unique way, since the kernel is the set of elements that map to the identity, and its complement is the set of elements that map to the generator of $\mathbb{Z}/2\mathbb{Z}$. The homomorphism is determined by choosing a value on each generator of the direct sum, so there are 2^n such homomorphisms, of which $2^n - 1$ are surjective: only the trivial homomorphism is not. Thus, there are $2^n - 1$ quadratic extensions. There are also $2^n - 1$ elements which are square roots of products of distinct primes with at least one prime in the product, and because those products are in a $\mathbb{Q}$-basis for K they give distinct quadratic extensions, so those quadratic extensions must comprise all quadratic extensions. $\square$