GEORGE MCNULTY

Groups and Fields

First Year Graduate Algebra
Part II
Homework Solutions

DRAWINGS BY THE AUTHOR

UNIVERSITY OF SOUTH CAROLINA

2015

Contents

PROBLEM SET 20

SOLVABILITY BY RADICALS AND OTHER THINGS GALOIS MAY HAVE KNOWN

PROBLEM 73.
Let p be prime and let H be a subgroup of S_p. Prove that if H has a transposition and an element of order p, then $H = S_p$. Provide an explicit counterexample when p is not prime.

SOLUTION
Let the p-element set to be permuted be $\{0, 1, 2, \ldots, p-1\}$. Without loss of generality, suppose $(0, 1) \in H$. Now any element of S_p of order p must be a p-cycle. Let τ be a p-cycle. Observe that it is always possible to pick k so that $\tau^k(0) = 1$. So without loss of generality, we can assume that $(0, 1, 2, \ldots, p-1) \in H$. Since we know that every premutation is a product of transpositions, it will suffice to show that every transposition can be generated by $(0, 1)$ and $(0, 1, 2, \ldots, p-1)$. Let us denote this p-cycle by τ. The following contentions are easy to establish by direct calculation.

Contention: $\tau(j, k)\tau^{-1} = (j+1, k+1)$ where the + works modulo p and $j \neq k$.

Contention: $(j, \ell)(j, k)(j, \ell) = (\ell, k)$ where j, k, and ℓ are distinct.

Contention: $\tau^\ell(j, k)\tau^{-\ell} = (j+\ell, k+\ell)$ where the + works modulo p and $j \neq k$.

According to the first two contentions, $(0, 1)$ and τ generate all transpositions of the form $(0, j)$. The last contention produces all the rest of the transpositions.

The contentions above hold, even if p is not prime. What breaks down in the composite case, is that τ^k need not be a p-cycle when $0 < k < p$. As a result we have no justification for assuming the given transposition transposes adjacent elements of the longer cycle.

Here is a counterexample for S_4. Let $\tau = (0, 1, 2, 3)$ be the 4-cycle and take $\sigma = (0, 2)$ as the transposition. Let $\gamma = (1, 3)$. We see that $\gamma = \tau\sigma\tau^{-1}$. We also see $\sigma = \tau\gamma\tau^{-1}$. We note, as well, that σ and γ are disjoint transpositions. This leads us to the following equations:

$$\sigma\gamma = \gamma\sigma$$
$$\tau\sigma = \gamma\tau$$
$$\tau\gamma = \sigma\tau$$

A direct calcultation gives us

$$\sigma\gamma = \tau^2$$

Recalling that τ has order 4 and transpositions have order 2, this leads us to the conclusion that the following 12 elements constitute a subgroup of S_4:

$$\begin{gathered}\tau^0, \tau^1, \tau^2, \tau^3\\ \sigma, \sigma\tau^1, \sigma\tau^2, \sigma\tau^3\\ \gamma, \gamma\tau^1, \gamma\tau^2, \gamma\tau^3\end{gathered}$$

But S_4 has 24 elements, so the subgroup generated by $(0,2)$ and $(0,1,2,3)$ is a proper subgroup.

PROBLEM 74.
Prove that $x^5 - 2x^3 - 8x + 2$ is not solvable by radicals over the field $\mathbb{Q}$ of rational numbers.

SOLUTION
Observe that this polynomial is irreducible according to Eisenstein and a Calculus I exercise shows that its derivative is 0 at $\pm\sqrt{2}$. It follows that the polynomial has three real roots, one less than $-\sqrt{2}$, one properly between $-\sqrt{2}$ and $\sqrt{2}$, and one greater than $\sqrt{2}$. The remaining roots must be nonreal complex numbers and, since the polynomial has real coefficients, these remaining roots must be complex conjugates. By a Fact proven in class, the Galois group of the polynomial must be S_5 (since 5 is prime). Since $5 > 4$ we know that this group is not solvable. So by Galois' Criterion, the polynomial is not solvable by radicals.

PROBLEM 75.
Let F be a finite field. Prove that the product of all the nonzero elements of F is -1. Using this, prove Wilson's Theorem:

$$(p-1)! \equiv -1 \pmod{p}$$

for every prime number p.

SOLUTION
Let q be the cardinality of F. We know that the elements of F are precisely the roots of $x^q - x$. This means that the roots of $x^{q-1} - 1$ are precisely the nonzero elements of F. Let the nonzero elements be $r_0, r_1, \ldots r_{q-2}$. Then $x^{q-1} - 1 = (x - r_0)(x - r_1)\ldots(x - r_{q-2})$. This tells us that -1 is the product of the nonzero elements of F. (The careful graduate student will realize that $(-1)^{q-1} = 1$ for all possible values of q.)

For the last bit, let $F = \mathbb{Z}_p$ where p is prime. The nonzero elements of this field are $1, 2, 3, \ldots, p-1$. Multiplication in $\mathbb{Z}_p$ is performed by forming the product in $\mathbb{Z}$ and then extracting the residue modulo p. In other words, Wilson's Theorem.

PROBLEM 76.

Let E be the splitting field of x^5-2 over the field $\mathbb{Q}$ of rationals. Find the lattice (draw a picture) of all fields intermediate between $\mathbb{Q}$ and E.

SOLUTION

Let ζ be a primitive 5th root of unity. Clearly, both $\sqrt[5]{2}$ (the real fifth root of 2) and $\sqrt[5]{2}\zeta$ are roots of x^5-2. So they belong to the splitting field E. Dividing, we see that $\zeta \in E$. It is evident that $\sqrt[5]{2}, \sqrt[5]{2}\zeta, \sqrt[5]{2}\zeta^2, \sqrt[5]{2}\zeta^3, \sqrt[5]{2}\zeta^4$ lists the five distinct roots of x^5-2. So $E=\mathbb{Q}[\sqrt[5]{2},\zeta]$.

To conserve notation we put

$$r_k := \sqrt[5]{2}\zeta^k \text{ for } 0 \le k < 5$$

So r_0, r_1, r_2, r_3, and r_4 are the five distinct roots of x^5-2 in E.

Observe that $[\mathbb{Q}[r_0]:\mathbb{Q}]=5$ since x^5-2 is irreducible over $\mathbb{Q}$ by Eisentstein. Also observe that $[\mathbb{Q}[\zeta]:\mathbb{Q}]=4$ since ζ is a root of $\lambda_5(x)$ which we know is irreducible over $\mathbb{Q}$ and has degree 4. Thus $[E:\mathbb{Q}]$ is divisible by both 5 and 4. This means $[E:\mathbb{Q}]$ is divisible by 20, since 4 and 5 are relatively prime. Now consider $\left[E:\mathbb{Q}[r_0]\right]$. Since ζ is a root of $\lambda_5(x)$, which has degree 4, we see that this dimension is no greater than 4. This means that $[E:\mathbb{Q}]$ is no larger than 20. So we find that $[E:\mathbb{Q}]=20$. It follows that $[\mathbb{Q}[\zeta,r_0]:\mathbb{Q}[r_0]]=4$. In turn, this entails that $\lambda_5(x)$ is irreducible over $\mathbb{Q}[r_0]$. We also get $\left[E:\mathbb{Q}[\zeta]\right]=5$. Since $E=\mathbb{Q}[r_0,\zeta]$ and r_0 is a root of the monic polynomial x^5-2, we see x^5-2 is irreducible over $\mathbb{Q}[\zeta]$.

Here are four obvious intermediate fields: $\mathbb{Q}, \mathbb{Q}[\zeta], \mathbb{Q}[r_0]$ and $E=\mathbb{Q}[\zeta,r_0]$. It is easy to see that these are all distinct. Clearly any field properly between $\mathbb{Q}$ and E must have dimension $2,4,5$, or 10. So the only remaining question is whether there are any others. There are.

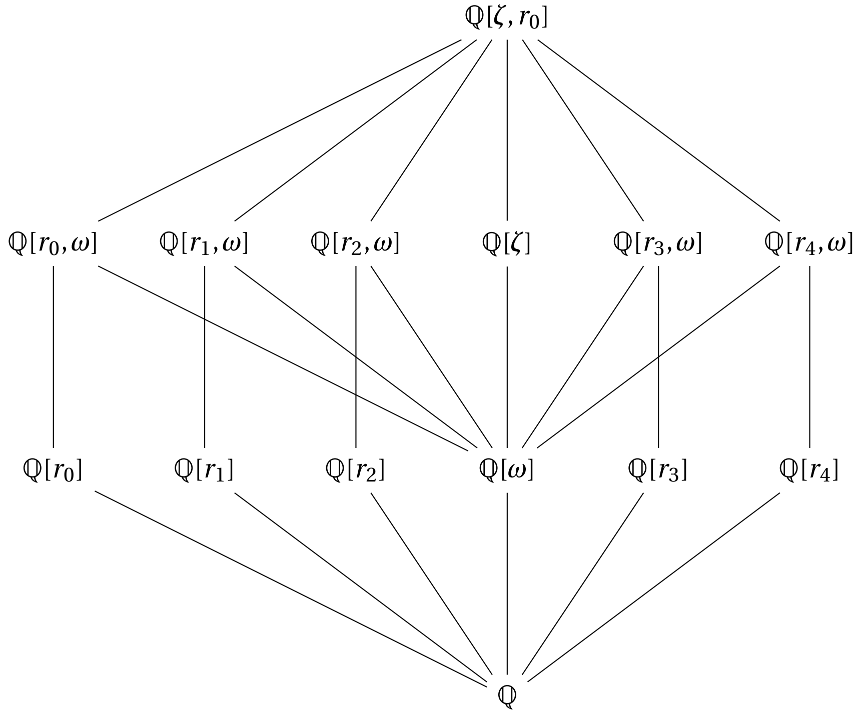
Since x^5-2 is irreducible over $\mathbb{Q}$ (by Eisenstein) Kronecker tells us that $\mathbb{Q}[r_k]$ is a subfield of E of dimension 5, when $0 \le k < 5$. No two of these fields can coincide, since given both $r_i = \sqrt[5]{2}\zeta^i$ and $r_j = \sqrt[5]{2}\zeta^j$ with $i \ne j$, after a bit of fiddling we can get both r_0 and ζ using just the field operations. So now we have at least five intermediate fields of dimension 5.

Now $\mathbb{Q}[\zeta]$ is the splitting field of the cyclotomic polynomial $\lambda_5(x)$ over $\mathbb{Q}$. This polynomial is irreducible over $\mathbb{Q}$ and has degree 4. So Kronecker tells us that it has dimension 4. So its Galois group has order 4. Kronecker also told us that the map that sends $\zeta \mapsto \zeta^2$ extends to a automorphism of $\mathbf{Q}[\zeta]$. This automorphism belongs to the Galois group and the automorphism is easily seen to have order 4. So the Galois group is the cyclic group of order 4. The subgroup lattice of this group is a three-element chain. By the Fundamental Theorem of Galois Theory, there will be exactly one field of dimension 2 sitting between $\mathbb{Q}$ and $\mathbb{Q}[\zeta]$. We know that conjugation, restricted to $\mathbb{Q}[\zeta]$ is the element of order 2. The field sitting properly between $\mathbb{Q}$ and $\mathbb{Q}[\zeta]$ is the fixed field of conjugation. Notice that $\zeta+\zeta^4=\zeta+\bar{\zeta}\notin\mathbb{Q}$, for otherwise $(x-\zeta)(x-\bar{\zeta})\in\mathbb{Q}[x]$ and it would be a factor of the irreducible polynomial $\lambda_5(x)$. But $\zeta+\bar{\zeta}$ is obviously fixed by conjugation. So, taking $\omega=\zeta+\bar{\zeta}$ we find the field of dimension 2 is $\mathbb{Q}[\omega]$. For reassurance, we note that x^2+x-1 is the minimal polynomial of ω.

Now let r be one of our five distinct roots of x^5-2. Since $\mathbb{Q}[r]$ has dimension 5 it follows that any irreducible polynomial in $\mathbb{Q}[x]$ of degree 2 (or 3) will also be irreducible over $\mathbb{Q}[r]$. By Kronecker, this means that $\mathbb{Q}[r,\omega]$ must have dimension 10 over $\mathbb{Q}$.

At this point, we have one field of dimension 1 (namely $\mathbb{Q}$), one field of dimension 2, one field of dimension 4, five fields of dimension 5, five fields of dimension 10 and one field of dimension 20.

Here is what the diagram looks like up to this point.



Can there be any other intermediate fields?

Let's invoke the Fundamental Theorem of Galois Theory. The Galois group $\mathrm{Gal}(E/\mathbb{Q})$ has cardinality 20 and it is embeddable into S_5. Here the underlying 5-element set is our five distinct roots of $x^5 - 2$. Notice that $\mathrm{Gal}(E/\mathbb{Q}[r_0])$ is a subgroup of $\mathrm{Gal}(E/\mathbb{Q})$. But $\mathrm{Gal}(E/\mathbb{Q}[r_0])$ is a cyclic group of order 4—the reasoning we used for $\mathrm{Gal}([\zeta]/\mathbb{Q})$ works here too. This means there is a 4-cycle permuting the nonreal roots. The uniqueness of splitting fields argument also gives us an automorphism of E that sends $r_0 \mapsto r_1$ which fixes ζ. This automorphism has order 5. So in $\mathrm{Gal}(E/\mathbb{Q})$ we have a 4-cycle and a 5-cycle. If you play around a bit, you will see that this generates a subgroup of order 20. After a while you can churn out all the subgroups and discover there are not more intermediate fields. There are even software programs for carrying out these kinds of group calculations.

A more sophisticated approach would find that there is one Sylow 5-subgroup and 5 Sylow 2-subgroups. In fact, Sylow tells us there are either 5 Sylow 2-subgroups or just 1. Certainly, there are no more. Since we already must have at least 5, Sylow tells us we have exactly 5. The Sylow 2-subgroups are all conjugate and so are isomorphic. Since we have an element of order 4, it follows that they are all copies of the cyclic group of order 4 and each has exactly one subgroup of order 2. Since every 2-subgroup is included in a Sylow 2-subgroup, we see that there are no more than 5 subgroups of order 2. But by our field analysis above, there are at least 5. We have in hand all possible subgroups, except those of order 10. A subgroup of order 10 must include the only subgroup of order 5 and it must have an element of order 2. There are exactly 5 elements of order 2. One of them is complex conjugation. Restricted to our 5 roots, it is the permutation $\sigma = (r_1, r_4)(r_2, r_3)$. Let $\tau = (r_0, r_1, r_2, r_3, r_4)$. An easy calculation shows

$$\sigma\tau^4 = \tau\sigma.$$

By way of this equation, any product of σ's and τ's in any order can be rearranged to obtain an element on the list of 10 distinct permutations below:

$$\tau^0, \tau, \tau^2, \tau^3, \tau^4, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3, \sigma\tau^4.$$

These elements comprise a subgroup of order 10. We would be done, if we can show that $\sigma\tau^k$ has order 2 for $0 \le k < 5$, since then the subgroup has all the elements of order 5 as well as all the elements of order

2. Straightforward calculations show

$$\begin{aligned}\sigma &= (r_1,r_4)(r_2,r_3)\\ \sigma\tau &= (r_0,r_4)(r_1,r_3)\\ \sigma\tau^2 &= (r_0,r_3)(r_1,r_2)\\ \sigma\tau^3 &= (r_0,r_2)(r_3,r_4)\\ \sigma\tau^4 &= (r_0,r_1)(r_2,r_4)\end{aligned}$$

and these all have order 2. So we have found the unique subgroup of order 10. So our lattice diagram above accounts for all the intermediate fields.

Problem 77.

Let F be a field of characteristic p, where p is a prime. Let E be a field extending F. Prove that E is a normal separable extension of F of dimension p if and only if E is the splitting field over F of an irreducible polynomial of the form $x^p - x - a$, for some $a \in F$.

Solution

$(\Leftarrow)$

Observe that $f(x) = x^p - x - a$ is a function with period 1. That is

$$f(x+1) = (x+1)^p - (x+1) - a = x^p + 1^p - x - 1 - a = x^p - x - a = f(x).$$

So if $u \in E$ is a root of $f(x)$ then all of $u, u+1, u+2, \dots, u+p-1$ are also roots and they are all distinct. This means that every root of $f(x)$ is really a primitive root of $f(x)$. So $E = F[u]$ where u is any root of $f(x)$. Since we are assuming that $f(x)$ is irreducible, Kronecker tells us that $[E:F] = \deg f(x) = p$. So all our desires are fulfilled by the Key Theorem.

$(\Rightarrow)$

Now we assume that E is a normal separable extension of F of dimension p over F. By the Key Theorem E is the splitting field of some separable polynomial over F and the Galois group $\mathrm{Gal}(E/F)$ is a cyclic group of cardinality p. Let $\mathrm{Id}, \sigma, \dots, \sigma^{p-1}$ be the elements of this Galois group. Problem 8 tells us that, as members of a vector space over E these maps are linearly independent. Hence

$$u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{p-1}(u)$$

cannot be 0 for every $u \in E$. So pick $u \in E$ so that

$$u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{p-1}(u) = b \neq 0.$$

Now notice that $\sigma(b) = \sigma(u) + \sigma^2(u) + \cdots + \sigma^{p-1}(u) + \sigma^p(u) = b$ since σ has order p. So b is fixed by each element of the Galois group. By the Fundamental Theorem of Galois Theory, $b \in F$. Now let

$$c = \sigma(u) + 2\sigma^2(u) + \cdots + (p-1)\sigma^{p-1}(u).$$

Then

$$\begin{aligned}\sigma(c) &= \sigma^2(u)+2\sigma^3(u)+\cdots+(p-2)\sigma^{p-1}(u)+(p-1)\sigma^p(u)\\ &= \sigma^2(u)+2\sigma^3(u)+\cdots+(p-2)\sigma^{p-1}(u)+(p-1)u\\ &= \sigma^2(u)+2\sigma^3(u)+\cdots+(p-2)\sigma^{p-1}(u)+(-1)(b-\sigma(u)-\sigma^2(u)-\cdots-\sigma^{p-1}(u))\\ &= \sigma(u)+2\sigma^2(u)+\cdots+(p-1)\sigma^{p-1}(u)-b\\ &= c-b\end{aligned}$$

Now put $v=-\frac{c}{b}$. From this we see

$$\sigma(v)=-\frac{\sigma(c)}{\sigma(b)}=-\frac{c-b}{b}=-\frac{c}{b}+1=v+1.$$

So, more generally, we see that $\sigma^k(v)=v+k$ for all natural numbers $k<p$.

Now put $a=v^p-v$. Observe

$$\sigma(a)=(\sigma(v))^p-\sigma(v)=(v+1)^P-(v+1)=v^p+1^p-v-1=v^p-v=a.$$

This means that a is fixed by all the members of the Galois group. So $a\in F$, since F is the fixed field of the Galois group. That is v is a root of $x^p-x-a\in F[x]$. Since the members of the Galois group fix the elements of F, the image of v under any one of these members must also be a root of x^p-x-a. So each $(x-(v+k))$ is a factor of x^p-x-a. It is not too hard to see that $x^p-x-a=\prod_{k<p}(x-(v+k))$.

If we could show that x^p-x-a is irreducible, then Kronecker would tell us that $[F[v]:F]=p=[E:F]$. So $E=F[v]$ and we would be done.

Now the minimal polynomial (over F) of v has degree $[F[v]:F]$. Since $F[v]=F[v+k]$ we see that the minimal polynomial of v and the minimal polynomial of $v+k$ (for any $k<p$) have the same degree. Also these minimal polynomials are factors of x^p-x-a and, in fact, must give the decomposition of x^p-x-a into its irreducible factors. So the common degree of the minimal polynomials must itself be a factor of the prime p. So either x^p-x-a is irreducible or else all those minimal polynomials have degree 1. In the latter case, $v\in F$. This is impossible since $\sigma(v)=v+1\neq v$, meaning that v is not fixed by σ and so cannot belong to the fixed field F.