some algebra prelim solutions*

David Morawski

August 19, 2012

Problem (Spring 2008, #5)**.** Show that $f(x) = x^p - x + a$ is irreducible over $\mathbb{F}_p$ whenever $a \in \mathbb{F}_p$ is not zero.

Proof. First, note that $f(x)$ has no roots in $\mathbb{F}_p$: since $b^p = b \mod p$ (Fermat's Little Theorem), $f(b) = b^p - b + a = a \neq 0$. Now, let α be a root of $f(x)$ in the algebraic closure of $\mathbb{F}_p$. Note that $\alpha + i$ for $i = 1, \ldots, p$ is also a root of $f(x)$. This is because in a field of characteristic p, we have $(x + y)^p = x^p + y^p$ for every x and y in the field; so

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) + a$$

becomes

$$\alpha^p + i^p - (\alpha + i) + a.$$

Again, by Fermat's Little Theorem, $i^p = i$, so this equation becomes

$$\alpha^p - \alpha + a,$$

which is zero by the assumption that α is a root. Thus, $\mathbb{F}_p(\alpha)$ contains every root of $f(x)$ and so

$$f(x) = \prod_{i=1}^{p} x - (\alpha + i)$$

over $\mathbb{F}_p(\alpha)$.

Now suppose, to the contradiction, that $f(x) = g(x)h(x) \in \mathbb{F}_p[x]$ such that $1 < \deg g(x) < p$. Then, letting $d = \deg g(x)$,

$$g(x) = \prod_{j=1}^{d} x - (\alpha + i_j)$$

over $\mathbb{F}_p(\alpha)$. Expanding this product shows that the coefficient of x^{d-1} is $-\sum_{j=1}^{d} \alpha + i_j$, which is equal to $-d\alpha + k$, for some $k \in \mathbb{F}_p$. Since $g(x)$ has coefficients in $\mathbb{F}_p$ and d is not zero, this means that α lies in $\mathbb{F}_p$, contradicting the fact that $f(x)$ has no roots in $\mathbb{F}_p$. □

*These solutions, chronologically listed, have not been checked by any prelim graders.

Problem (Fall 2008, #2)**.** Prove that if a polynomial f in $k[x]$ with a field k has a repeated irreducible factor g in $k[x]$, then g divides the greatest common divisor of f and its derivative. Be sure to explain what *derivative* can mean without limits.

Proof. First, let's define the *algebraic* derivative of a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ in $k[x]$. We define the map $D : k[x] \to k[x]$ on the k-basis of $k[x]$ by $Dx^n = nx^{n-1}$ and extend k-linearly. To see if the product rule holds, we evaluate D on the product of two basis elements:

$$D(x^n x^m) = Dx^{n+m} = (n+m)x^{n+m-1}.$$

On the other hand:

$$Dx^n \cdot x^m + x^n \cdot Dx^m = nx^{n-1}x^m + mx^n x^{m-1} = (n+m)x^{n+m-1}.$$

Since the product rule holds on the basis elements and D is k-linear, it holds for all polynomials in $k[x]$.

Note that $D1 = D(1 \cdot 1) = D1 \cdot 1 + 1 \cdot D1$, so $D1 = 0$. Extending k-linearly, this means that the derivative of any constant polynomial is zero (which was left a bit ambiguous in our definition). Conversely, if $D(a_n x^n + a_{n-1}x^{n-1} + \cdots) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots = 0$ in a field with characteristic not dividing n, then it must be that $n = 0$.

Now suppose $f(x) = g(x)^n h(x)$, where $n > 1$ and g is irreducible. g certainly divides f, so we just need to show that g also divides Df. We compute Df:

$$Df = D(g^n h) = Dg^n \cdot h + g^n \cdot Dh = ng^{n-1}h + g^n Dh.$$

If the characteristic of k divides n, then $Df = g^n Dh$ and we have that g divides both f and Df. If the characteristic of k does not divide n, then the irreducibility of g means that g is nonconstant (any constant is a unit in $k[x]$, since k is a field), so $Dg \neq 0$. By assumption, $n - 1 > 0$, so we can factor out $g(x)$ from Df, giving us:

$$Df = g(ng^{n-2}h + g^{n-1}Dh).$$

So g divides Df. So, in any characteristic, g must divide the greatest common divisor of f and Df. □

Problem (Fall 2009, #7)**.** Show that $f(z) = wz^4 - 4z + 1 = 0$ has multiple roots z only for $w = 27$.

Proof. A multiple root α of $f(z)$ is also a root of the algebraic derivative[1] $Df(z) = 4wz^3 - 4$. I.e.,

$$4w\alpha^3 - 4 = 0,$$

which means that $w = \alpha^{-3}$. So, plugging α into f gives us

$$f(\alpha) = \alpha^{-3}\alpha^4 - 4\alpha + 1 = 0,$$

which simplifies to $\alpha = 1/3$. So $w = \alpha^{-3} = (1/3)^{-3} = 27$, as we wished to show. □

[1] I'm assuming that we're working over a field, although the problem does not say so.

Problem (Spring 2010, #5)**.** Let R be a commutative ring of endomorphisms of a finite-dimensional complex vector space V. Prove that there is at least one (non-zero) common eigenvector for R on V.

Proof. Let W be the $\mathbb{C}$-linear span of R. So, W is a subspace of $\mathrm{End}_{\mathbb{C}}(V)$, hence finite-dimensional since V is. By definition, every vector in W is a $\mathbb{C}-$linear combination of elements of R. So, because the elements of R commute, W is also commutative (with respect to composition). Let $T_1, \ldots, T_n$ be a basis for W. Let's now show that we can find a simultaneous eigenvector for this basis.

We induct on n: for $n = 1$, T_1 has an eigenvector since $\mathbb{C}$ is algebraically closed. Hence, the minimal polynomial for T_1 has a root over $\mathbb{C}$, which is an eigenvalue corresponding to a nonzero eigenvector.

Now assume $T_1, \ldots, T_{n-1}$ have a simultaneous eigenvector, say $v \in V$ with $T_i v = \lambda_i v$. Letting V_{λ_i} denote the λ_i-eigenspace for T_i where $1 \leq i < n$, we show that the intersection $\cap_{i=1}^{n-1} V_{\lambda_i}$ is T_n-stable. Indeed, a vector w in the intersection lies in each V_{λ_i}, so $T_i w = \lambda_i w$ for $1 \leq i < n$. So,

$$T_i T_n w = T_n T_i w = T_n \lambda_i w = \lambda_i T_n w,$$

since $T_i T_n = T_n T_i$. So $T_n w$ lies in each V_{λ_i}, hence lies in the intersection. Now, since the intersection $\cap_{i=1}^{n-1} V_{\lambda_i}$ is T_n-stable, it makes sense to speak of the minimal polynomial for T_n of this subspace. Once again, since $\mathbb{C}$ is algebraically closed, this polynomial has a root, which precisely corresponds to an eigenvector v' for T_n. Since v' lies in $\cap_{i=1}^{n-1} V_{\lambda_i}$, it is simultaneously an eigenvector for the entire basis $T_1, \ldots, T_n$, say with respective eigenvalues γ_i.

Now it just remains to show that v' is a simultaneous eigenvector for R. If r is any element of R, then

$$r = \sum_{i=1}^{n} a_i T_i$$

for a_i in $\mathbb{C}$. So,

$$r(v') = (\sum a_i T_i)(v') = \sum a_i T_i(v') = \sum a_i \gamma_i v' = (\sum a_i \gamma_i) v'$$

Thus, v' is an eigenvector for each R. □

Problem (Fall 2010, #3)**.** Show that $f(x) = x^{25} - 10$ factors linearly over $\mathbb{F}_{101}$, the field of 101 elements.

Proof. Note that $10^4 = 100 \cdot 100 = (-1)(-1) = 1 \mod 101$. So 10 is a root of $f(x)$ since

$$10^{25} = 10^{24} \cdot 10 = 1 \cdot 10 = 10.$$

Now consider $\mathbb{F}_{101}^{\times}$, which is cyclic of order 100. Since 25 divides 100, there is an element α of order 25. For $j = 0, 1, \ldots, 24$, we have

$$(10 \cdot \alpha^j)^{25} = 10^{25} \cdot (\alpha^{25})^j = 10,$$

giving 25 roots of $f(x)$. And each α^j is distinct since $\{1, \alpha, \alpha^2, \ldots, \alpha^{24}\}$ is the cyclic group generated by α. Combining this with the fact that 10 is invertible, it follows that these 25 roots are distinct. So $f(x)$ splits into linear factors. □

Problem (Fall 2010, #5)**.** Let X, Y be $n-$by$-n$ complex matrices such that $XY = YX$. Suppose that there are $n-$by$-n$ invertible matrices A, B such that AXA^{-1} and BYB^{-1} are diagonal. Show that there is an $n-$by$-n$ invertible matrix C such that CXC^{-1} and CYC^{-1} are diagonal.

Proof. First we prove that the existence of matrices A and B is equivalent to X and Y each having a basis of eigenvectors. To see this, let $D = AXA^{-1}$. Then $De_i = \lambda_i$ for each i, since D is diagonal. From $D = AXA^{-1}$, we get that $XA^{-1} = A^{-1}D$. So

$$XA^{-1}e_i = A^{-1}De_i = A^{-1}\lambda_i e_i = \lambda_i A^{-1}e_i.$$

So $A^{-1}e_i$ is an eigenvector for X. Because A^{-1} is an isomorphism, the vectors $\{A^{-1}e_i\}_{i=1,\ldots,n}$ are a basis for $\mathbb{C}^n$, thus an eigenbasis.

Conversely, suppose X has an eigenbasis $v_1, \ldots, v_n$ for $\mathbb{C}^n$ with $Xv_i = \lambda_i v_i$. Let P be the matrix such that the i^{th} column of P is v_i. Then P has full rank, hence P^{-1} exists. Furthermore, $P^{-1}XP$ is diagonal, since

$$P^{-1}XPe_i = P^{-1}Xv_i = P^{-1}\lambda_i v_i = \lambda_i P^{-1}v_i = \lambda_i e_i,$$

So, there is a matrix, namely P^{-1}, such that conjugating X with P^{-1} yields a diagonal matrix.

Returning to the original problem, we see that X and Y both have an eigenbasis for $\mathbb{C}^n$ (i.e., are diagonalizable). Then $\mathbb{C}^n = \bigoplus V_\lambda$, the direct sum of distinct eigenspaces of X. Since X and Y commute, each V_λ is Y-stable.

Let's show that for a diagonalizable linear operator T on a finite dimensional vector space V over a field k, whenever $W \subset V$ is T-stable, T is diagonalizable on W. Let $f(x)$ be the minimal polynomial for T on V over k. Since W is T-stable, it makes sense to speak about the minimal polynomial $g(x)$ for T on W. Since $f(T)(V) = 0$, $f(T)(W) = 0$. Thus, by definitely of $g(x)$, $g(x)$ divides $f(x)$. And because T is diagonalizable, $f(x)$ splits into distinct linear factors. Then so does $g(x)$ and, hence, T is diagonalizable on W.

So each V_λ has a basis of eigenvectors for Y. And because these vectors lie in V_λ, they are eigenvectors for X. Taking the union of these vectors gives us a basis for $\mathbb{C}^n$ that are simultaneously eigenvectors for $\mathbb{C}^n$. Then, from what we saw above, letting these vectors be the columns of a matrix C, we have that $C^{-1}XC$ and $C^{-1}YC$ are diagonal. □

Problem (Fall 2011, #1)**.** Describe all abelian groups of order 72.

Proof. By the Fundamental Theorem of Finite Abelian Groups, any group G of order 72 is isomorphic to the direct product of cyclic groups of prime power order, unique up to reordering. Also, by Sun-Ze's theorem, we may collapse the direct product cyclic groups

$\mathbb{Z}/m \times \mathbb{Z}/n$ to $\mathbb{Z}/mn$ whenever m and n are relatively prime. That said, we enumerate all abelian groups of order $72 = 2^3 \cdot 3^2$:

$$\begin{aligned}
\mathbb{Z}/8 \times \mathbb{Z}/9 &\cong \mathbb{Z}/72 \\
\mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/3 &\cong \mathbb{Z}/24 \times \mathbb{Z}/3 \\
\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/9 &\cong \mathbb{Z}/4 \times \mathbb{Z}/18 \\
\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 &\cong \mathbb{Z}/12 \times \mathbb{Z}/6 \\
\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 &\cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/18 \\
\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 &\cong \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/6
\end{aligned}$$

□

Problem (Fall 2011, #5)**.** Prove that the ideal generated by 7 and $x^2 + 1$ is maximal in $\mathbb{Z}[x]$.

Proof. Let M denote the ideal generated by 7 and x^2+1. To show that M is maximal, we'll show that $\mathbb{Z}[x]/M$ is a field. Note that

$$\mathbb{Z}[x]/M \cong (\mathbb{Z}[x]/7)/(x^2+1) \cong (\mathbb{Z}/7)[x]/(x^2+1).$$

So $\mathbb{Z}[x]/M$ is a field if and only if $(\mathbb{Z}/7)[x]/(x^2+1)$ is a field. Since $\mathbb{Z}/7$ is a field, $(\mathbb{Z}/7)[x]$ is a unique factorization domain. Now notice that because x^2+1 has no roots (a root would have order 4 in $(\mathbb{Z}/7)^\times$, which is impossible by Lagrange) in $\mathbb{Z}/7$, it is irreducible. But in a unique factorization domain, this means that x^2+1 is prime and generates a prime ideal. So $(\mathbb{Z}/7)[x]/(x^2+1)$ is an integral domain. But it is a *finite* integral domain, so it is a field. □

Problem (Spring 2012, #1)**.** Show that all groups of order 35 are cyclic.

Proof. Let G be a group of order $35 = 3 \cdot 7$. By Sylow's theorem, the number of 5-Sylow subgroups is equal to 1 modulo 5 and also must divide 35. The only number satisfying these conditions is 1. So there is a unique 5-Sylow subgroup H. Furthermore, since p-Sylow subgroups are conjugate to one another, H being the unique 5-Sylow subgroup means that H must be normal in G. Similarly, the number of 7-Sylow subgroups is equal to 1 modulo 7 and must divide 35. Again, the only possibility is that there is a unique (hence normal) 7-Sylow subgroup K. Note that if x is an element of both H and K, then Lagrange tells us that $x^5 = 1 = x^7$. So the order of x divides both 5 and 7, thus the order of x must be 1. Thus, $H \cap K = 1$.

Since H and K are normal and $H \cap K = 1$, we have that

$$HK \cong H \times K \cong \mathbb{Z}/5 \times \mathbb{Z}/7.$$

And because 5 and 7 are relatively prime, $\mathbb{Z}/5 \times \mathbb{Z}/7 \cong \mathbb{Z}/35$. So HK is a subgroup of G of order 35, so HK equals G. So G is isomorphic to $\mathbb{Z}/35$. □

Problem (Spring 2012, #2)**.** Let G be a finite group and H a subgroup of index 2. Show that H is normal.

Proof. By definition, the index of H in G is the number of left cosets of H, which is the same as the number of right cosets of H. Thus, there are two left cosets: H and gH, where g does not lie in H. Because these two sets are disjoint and their union is G, $gH = G - H$. Similarly, $Hg = G - H$. So $gH = Hg$ for all g, which is exactly the statement that H is normal. □