(*April 4, 2005*)

Homework 17, due Wed Mar 23

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[17.1] Give generators for the $p+1$ subgroups of order p of the group $A = \mathbf{Z}/p \oplus \mathbf{Z}/p$, where p is prime.

Granting that the count of such subgroups is $p+1$ (for example, as an easy case of the following exercise), we claim that $(1,0)$, $(1,1)$, $(1,2)$, ..., $(1,p-1)$, $(0,1)$ generate these subgroups. Indeed, if

$$n \cdot (a,b) = (c,d)$$

then $na = c$ and $nb = d$, and $ad = bc$. Our choices exactly precluded this. ///

[17.2] Let p be a prime. Let $1 \le k \le n$. How many subgroups of order p^k are there of $(\mathbf{Z}/p)^n$?

Count these by taking into account the fact that $V = (\mathbf{Z}/p)^n$ is a vectorspace over the field $K = \mathbf{Z}/p$, and we are asking for k-dimensional subspaces. Thus, we choose subspaces by choosing ordered bases for the subspaces, and then divide by the number of different ordered bases of a k-dimensional subspace.

There are $p^n - 1$ choices of non-zero vector v_1 for first basis element. For each choice of v_1, there remain $p^n - p$ choices for the second basis element v_2, namely vectors not lying in the span of v_1. For each choice of v_1, v_2, there remain $p^n - p^2$ choices for the third basis element v_3, namely vectors not lying in the span of v_1, v_2. (Since v_1, v_2 are linearly independent by construction, this span is 2-dimensional.) Thus, continuing in this vein, there are

$$(p^n-1)(p^n-p)(p^n-p^2)(p^n-p^3)\ldots(p^n-p^{k-1})$$

choices of ordered basis for k-dimensional subspaces. Similarly, the number of ordered bases of a fixed k-dimensional subspace is counted as

$$(p^k-1)(p^k-p)(p^k-p^2)(p^n-p^3)\ldots(p^k-p^{k-1})$$

Thus, the number of k-dimensional subspaces of an n-dimensional space over $\mathbf{F}_p$ is

$$\frac{(p^n-1)(p^n-p)(p^n-p^2)(p^n-p^3)\ldots(p^n-p^{k-1})}{(p^k-1)(p^k-p)(p^k-p^2)(p^n-p^3)\ldots(p^k-p^{k-1})}$$

It is not obvious, but replacing k by $n-k$ does not change the value of this expression. ///

[17.3] Give explicit generators for the 4 cubic subfields of $\mathbf{Q}(\zeta_{91})$, where ζ_{91} is a primitive 91^{st} root of unity.

Inside the big cyclotomic field are the smaller ones $\mathbf{Q}(\zeta_7)$ and $\mathbf{Q}(\zeta_{13})$, where $\zeta_7 = \zeta_{91}^{13}$ and $\zeta_{13} = \zeta_{91}^{7}$. (Note that *these* exponentiations are *not* automorphisms of the field!) There are the two *obvious* cubic subfields

$$\mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbf{Q}(\zeta_7)$$

$$\mathbf{Q}(\zeta_{13} + \zeta_{13}^{5} + \zeta_{13}^{5^2} + \zeta_{13}^{5^3}) \subset \mathbf{Q}(\zeta_{13})$$

using the cyclic subgroup of order 4 of $(\mathbf{Z}/13)^\times$ generated by 5.

We know that

$$\text{Aut}(\mathbf{Q}(\zeta_{91})/\mathbf{Q}) \approx (\mathbf{Z}/91)^\times \approx (\mathbf{Z}/7)^\times(\mathbf{Z}/13)^\times \approx \mathbf{Z}/6 \oplus \mathbf{Z}/12 \approx \mathbf{Z}/2 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/4$$

by

$$\sigma_a \longleftarrow a$$

where

$$\sigma_a(\zeta_{91}) = \zeta_{91}^a$$

By the main theorem of Galois theory, cubic extensions of $\mathbf{Q}$ inside $\mathbf{Q}(\zeta_{91})$ correspond to subgroups of index 3. Since the group is abelian, any such group must contain the subgroup $\mathbf{Z}/2 \oplus \mathbf{Z}/4$ of order 8, and then a further choice of subgroup of order 3.

The isomorphism $(\mathbf{Z}/7)^\times \times (\mathbf{Z}/13)^\times$ is realized via an effective form of Sun-Ze's theorem by

$$(a \bmod 7,\ b \bmod 13) \to b \cdot 2 \cdot 7 + a \cdot (-1) \cdot 13 = 14b - 13a \bmod 91$$

since

$$2 \cdot 7 + (-1) \cdot 13 = 1$$

The subgroup of order 2 in $(\mathbf{Z}/7)^\times$ is generated by -1, and the subgroup of order 4 in $(\mathbf{Z}/13)^\times$ is generated by 5. The images of $(-1, 1)$ and $(1, 5)$ in $(\mathbf{Z}/91)^\times$ are, respectively, $-14 - 13 = 64$ and $56 - 13 = 43$. Thus, the element

$$\alpha = \sum_{i=0,1} \sum_{j=0,1,2,3} \zeta_{91}^{64^i \cdot 43^j}$$

lies inside a field of degree 9 over $\mathbf{Q}$ whose Galois group over $\mathbf{Q}$ is

$$(\mathbf{Z}/91)^\times/(\text{copy of})(\mathbf{Z}/2 \oplus \mathbf{Z}/4) \approx \mathbf{Z}/3 \oplus \mathbf{Z}/3$$

From an earlier example, the powers ζ_{91}^ℓ with ℓ in the range $1 \le \ell < 91$ and $\gcd(\ell, 91) = 1$ are linearly independent over $\mathbf{Q}$, and thus this α is *not* accidentally in a smaller field.

The elements $(2, 1)$ and $(1, 3)$ generate the group isomorphic to $\mathbf{Z}/3 \oplus \mathbf{Z}/3$ inside $(\mathbf{Z}/91)^\times$, and their images in

$$\text{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q}) \approx \text{Gal}(K/\mathbf{Q})/\text{Gal}(K/\mathbf{Q}(\alpha)$$

thus generate the Galois group G of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$. This group G is isomorphic to $\mathbf{Z}/3 \oplus \mathbf{Z}/3$, but the automorphisms' indices are better written multiplicatively. Thus, the $3 + 1 = 4$ subgroups of G are (respectively) generated by

$$(2, 1)^a \cdot (1, 3)^b = (2^a, 3^b) \to 14 \cdot 3^b - 13 \cdot 2^a \bmod 91$$

where $(a, b) = (1, 0)$, $(1, 1)$, $(1, 2)$, and $(0, 1)$. The respective elements mod 91 are

$$c = \begin{cases} (2,1) & \to & 14 \cdot 1 - 13 \cdot 2 & = & 79 \bmod 91 \\ (2,3) & \to & 14 \cdot 3 - 13 \cdot 2 & = & 16 \bmod 91 \\ (2,9) & \to & 14 \cdot 9 - 13 \cdot 2 & = & 9 \bmod 91 \\ (1,3) & \to & 14 \cdot 3 - 13 \cdot 1 & = & 29 \bmod 91 \end{cases}$$

Then further averaging α over these groups of order 3 gives (with the same linear independence over $\mathbf{Q}$ as earlier) 4 generators (with $c = 79, 16, 9, 29$ as just computed)

$$\sum_{\ell=0,1,2} \sigma_c^\ell(\alpha) = \sum_{\ell=0,1,2} \sigma_c^\ell \left(\sum_{i=0,1} \sum_{j=0,1,2,3} \zeta_{91}^{64^i \cdot 43^j} \right) = \sum_{\ell=0,1,2} \sum_{i=0,1} \sum_{j=0,1,2,3} \zeta_{91}^{64^i \cdot 43^j \cdot c^\ell}$$

Remark: Since we can find the first two cubic fields relatively easily, in the sense that we can determine the minimal polynomial for generators without too much computational travail (not from these last expression, though!), we could also find minimal polynomials for the other two cubics by computations within the nonic extension K. ///

[17.4] Suppose K is a *normal* cubic field over $\mathbf{Q}$, generated by an element α with minimal polynomial $f(x) \in \mathbf{Q}[x]$. Explain without computing why it is that the discriminant of f is a square in $\mathbf{Q}$.

The minimal polynomial of α is necessarily irreducible. Since $\mathbf{Q}(\alpha)$ is normal over $\mathbf{Q}$, any map $\mathbf{Q}(\alpha) \to \overline{\mathbf{Q}}$ has the same image. In particular, the other two zeros β, γ of $f(x)$ lie in K. Thus,

$$(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) \in K$$

And

$$\Delta = \left((\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)\right)^2 \in \mathbf{Q}$$

since this is a symmetric expression in the roots. If Δ were *not* a square in $\mathbf{Q}$, then K would contain the quadratic extension $\mathbf{Q}(\sqrt{\Delta})$ of $\mathbf{Q}$. By the multiplicativity of field extension degrees in towers, this would imply that

$$3 = [K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{D})] \cdot [\mathbf{Q}(\sqrt{D}) : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{D})] \cdot 2$$

which is impossible since degrees are integers. ///

[17.5] Give an example of two commuting diagonalizable operators S, T on a 4-dimensional vectorspace V over a field k such that each operator has exactly two eigenvalues, and the eigenspaces are two-dimensional, but/and the intersection of any S-eigenspace with any T-eigenspace is just 1-dimensional. Explain why this does not contradict results about simultaneous eigenvectors.

Let

$$S = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix}$$

act on $V = k^4$ (column vectors). Then the standard basis elements $e_1.e_2.e_3.e_4$ are the joint eigenvectors for S and T, with four different ordered pairs of eigenvalues.

The too-naive assertion that for commuting endomorphisms S, T the eigenvectors of S are eigenvectors for T is contradicted by this example, since any vector $ae_1 + be_2$ (with $a, b \in k$) is an eigenvector for S, but not for T unless $ab = 0$.

But, of course, this is perfectly fine, since there is still a basis consisting of joint eigenvectors. The point is that it is unwise to hastily choose a basis of eigenvectors for one operator, hoping or presuming that they'll be eigenvectors for the other operator. For example, $e_1 + e_2$, e_2, e_3, e_4 is a basis consisting of S-eigenvectors, but the first of these is not an eigenvector for T. ///

[17.6] Let T be a diagonalizable operator on a finite-dimensional vector space V over a field k. Suppose that some T-eigenspace is not one-dimensional. Exhibit a diagonalizable endomorphism S of V commuting with T *not* lying in $k[T]$.

Let $P \in k[T]$ be the projector to the λ-eigenspace V_λ of T, with $\dim V_\lambda > 1$. Let A be a non-scalar endomorphism of V_λ. Such A exists exactly because $\dim V_\lambda > 1$. Then take $S = A \circ P$. This commutes with T, because for any $v \in V$

$$ST(v) = (AP)T(v) = A(TPv) = A(\lambda \cdot Pv) = \lambda \cdot APv = T(APv)$$

since $APv \in V_\lambda$. Yet, given a polynomial $f(x)$, take $v \in V_\lambda$, and compute

$$f(T)(v) = f(\lambda) \cdot v$$

so $f(T)$ is a scalar operator on V_λ. Thus, S is not of the form $f(T)$. ///

[17.7] Let $\lambda_1, \ldots, \lambda_n$ be distinct elements of a field k. Let $\mu_1, \ldots, \mu_n$ be arbitrary elements of k. Show that there is a unique polynomial $f(x)$ in $k[x]$ of degree $\leq n - 1$ such that $f(\lambda_i) = \mu_i$ for all i.

[This is Lagrange interpolation again.]

[17.8] Let T be a diagonalizable operator on a finite-dimensional vector space V over a field k. Suppose that all the eigenspaces are one-dimensional. Prove that any endomorphism commuting with T is in $k[T]$.

We know that an endomorphism S commuting with T stabilizes the eigenspaces of T. Since each eigenspace V_λ is just one-dimensional, S acts by a scalar μ_λ on V_λ. Let $f(x)$ be the minimal polynomial of T, and $f_\lambda(x) = f(x)/(x-\lambda)$. These polynomials have *gcd* 1, so there are polynomials $a_\lambda(x)$ such that

$$1 = \sum_\lambda a_\lambda(x) \cdot f_\lambda(x)$$

As observed in the notes and in class,

$$\mathrm{id}_V = \sum_\lambda a_\lambda(T) \cdot f_\lambda(T)$$

and $f_\lambda(T)$ is 0 on V_μ for $\mu \neq \lambda$. Further, $P_\lambda = a_\lambda(T) f_\lambda(T)$ is in $k[T]$ and is the projector to V_λ. Then

$$S = \sum_\lambda \mu_\lambda \cdot P_\lambda \in k[T]$$

as claimed. ///

[17.9] Let S, T be commuting diagonalizable endomorphisms of a finite-dimensional vector space V over a field k. Suppose that there is a basis $\{v_1, \ldots, v_n\}$ of simultaneous eigenvectors such that for $i \neq j$ the two vectors v_i and v_j either have different eigenvalues for S or have different eigenvalues for T. Show that there is a single diagonalizable operator R on V such that $k[S,T] = k[R]$.

Let $P_\lambda \in k[S]$ be the projector to the λ-eigenspace of S, and $Q_\mu \in k[T]$ the projector to the μ-eigenspace of T. Since S and T commute, $P_\lambda Q_\mu = Q_\mu P_\lambda$ is a projector commuting with both S and T. We claim that $P_\lambda Q_\mu$ is the projector to the joint eigenspace where S is λ and T is μ. Certainly Q_μ maps the whole space to the μ eigenspace for T. Since P_λ commutes with T, it stabilizes this eigenspace, so $(P_\lambda Q_\mu)(V)$ is contained in the μ-eigenspace of T. Symmetrically, it is contained in the λ eigenspace for S, so is contained in the joint eigenspace. On the other hand, for a joint eigenvector v with $Sv = \lambda v$ and $Tv = \mu v$, we have

$$(P_\lambda Q_\mu)(v) = P_\lambda(Q_\mu v) = P_\lambda(v) = v$$

In the form the question is asked, let v_i have eigenvalue λ_i for S and μ_i for T. Then $E_i = P_{\lambda_i} Q_{\mu_i}$ is a family of mutually orthogonal projectors (meaning that $E_i E_j = 0$ unless $i = j$, in which case it is E_i), whose sum is the identity endomorphism on V.

Now **assume** that there are at least n distinct elements $\alpha_1, \ldots, \alpha_n$ in the field k, and let

$$R = \sum_i \alpha_i \cdot E_i \in k[S,T]$$

By arrangement R is diagonalizable and has one-dimensional eigenspaces. Since S and T commute with R, by an earlier example both S and T are in $k[R]$. Thus, $k[R] = k[S,T]$. ///

[17.10] Give an example of a diagonalizable operator T on a 2-dimensional complex vector space V (with hermitian inner product $\langle , \rangle$) with eigenvectors v, w such that application of the Gram-Schmidt process does *not* yield two orthonormal *eigenvectors*.

Let $V = \mathbf{C}^2$ (column vectors) with the usual hermitian inner product, and let $T = \begin{pmatrix} 1 & 1 \\ 02 & \end{pmatrix}$. It has eigenvectors $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (eigenvalue 1) and $v_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ (eigenvalue 2). These are not orthogonal to each other. If we apply Gram-Schmidt, instead of v_2 we have

$$v_2' = v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} \cdot v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The latter vector is not an eigenvector. ///

[17.11] Let S be a hermitian operator on a finite-dimensional complex vector space V with hermitian inner product $\langle , \rangle$. Let W be a S-stable subspace of V. Show that S is hermitian on W.

Let S_o be the restriction of S to W. If we show that for all $w, w' \in W$

$$\langle S_o w, w' \rangle = \langle w, S_o w' \rangle$$

then by the *uniqueness* of adjoints $S_o^* = S_o$. Indeed, because

$$\langle Sw, w' \rangle = \langle w, Sw' \rangle$$

for w, w' in the *whole* space V, the identity certainly holds for $w, w' \in W$. ///

Remark: In a similar vein, one can directly show more generally that, for a *normal* endomorphism T on V stabilizing a subspace W, the restriction of T^* to W is the adjoint of the restriction of T to W.

[17.12] Let S, T be commuting hermitian operators on a finite-dimensional complex vector space V with hermitian inner product $\langle , \rangle$. Show that there is an orthonormal basis for V consisting of simultaneous eigenvectors for both S and T.

First, the Spectral Theorem for S says that V is the *orthogonal* direct sum of the eigenspaces V_λ for S. We know that T stabilizes each such eigenspace. From the previous example, the restriction of T to each V_λ is still hermitian, so on each V_λ there is an orthonormal basis $\{e_i^\lambda\}$ consisting of eigenvectors for T (and λ-eigenvectors for S). Then, since the different eigenspaces V_λ are mutually orthogonal, the aggregate $\{e_i^\lambda\}$ is an orthonormal basis for all of V. ///