# MODULAR FORMS EXAMPLE SHEET 3

1. Let $K$ be a field and let $A$ be a finite dimensional $K$-algebra; that is, a ring containing $K$ that is finite dimensional as a $K$-vector space.

1a. Show that every prime ideal of $A$ is maximal.

Let $\mathfrak{p}$ be a prime of $A$. Then $A/\mathfrak{p}$ is a domain which is finite-dimensional as a $K$-vector space; it suffices to show that such a ring is a field (as then $\mathfrak{p}$ will be maximal.) Let $x$ be a nonzero element of $A/\mathfrak{p}$, and let $I$ be the ideal: $\{P \in K[t] : P(x) = 0\}$ in $K[x]$. The ideal $I$ contains more than just the zero polynomial, as the infinite set $1, x, x^2, \ldots$ must be $K$-linearly dependent in $A/\mathfrak{p}$. Let $P$ be a generator for $I$. Then $P$ is not divisible by $t$ (since if it were then $P(t)/t$ would also be in $I$), and so has nonzero constant term: $P(t) = tQ(t) + c$. Then we have $xQ(x) = c$ in $A/\mathfrak{p}$, and so $x$ is a unit since $c$ is.

1b. Show that if $A$ contains no nonzero nilpotent elements, then $A$ is a product of finite extensions of $K$. [You may use, without proof, the result that an element $r$ of a ring $R$ is nilpotent if, and only if, $r$ is contained in every prime ideal of $R$. For a proof of this fact, see for instance Eisenbud, *Commutative Algebra*, pp. 70-71.]

Consider the map:

$$f : A \to \prod_{\mathfrak{p}} A/\mathfrak{p},$$

where $\mathfrak{p}$ runs over the prime ideals of $A$. The right-hand side is a product of fields by 1a, and each such field is a finite-dimensional $K$-vector space. It thus suffices to show that $f$ is an isomorphism. On the other hand $f$ is injective as its kernel is the intersection of all prime ideal $\mathfrak{p}$, and any element of this intersection is nilpotent. So it suffices to show that $f$ is surjective.

Fix any prime $\mathfrak{p}$. For each $\mathfrak{p}'$ different from $\mathfrak{p}$ there is an element $x_{\mathfrak{p}'}$ that lies in $\mathfrak{p}'$ but not $\mathfrak{p}$ (as both are maximal, so neither contains the other). Let $y_{\mathfrak{p}}$ be the product of the $x_{\mathfrak{p}'}$. Then $y_{\mathfrak{p}}$ maps to a nonzero element $\alpha$ of $A/\mathfrak{p}$ but maps to zero in each $A/\mathfrak{p}'$. Let $\beta$ be an element of $A$ that maps to $\alpha^{-1}$ in $A/\mathfrak{p}$, and set $z_{\mathfrak{p}} = \beta y_{\mathfrak{p}}$. Thus the image of $z_{\mathfrak{p}}$ under $f$ is 1 in the factor $A/\mathfrak{p}$ and zero in all the other factors. It follows that $f$ is surjective as required.

1c. Let $V$ be a finite dimensional vector space over an algebraically closed field $K$, and let $T_1, T_2, \ldots$ be a collection of commuting linear operators on $V$. Show that $V$ admits a basis of common eigenvectors for the $T_i$ if, and only if, there is no polynomial in the $T_i$ (with coefficients in $K$) that is a nonzero nilpotent endomorphism of $V$. [Hint: Let $A$ be the subring of

$\mathrm{End}(V)$ consisting of all polynomials in the $T_i$ with coefficients in $K$, and use 1b.]

Let $A$ be as in the hint, and note that a basis of simultaneous eigenvectors for the $T_i$ is a basis of simultaneous eigenvectors for every element of $A$. If $A$ contains a nilpotent $T$, then $T$ is a nilpotent with a basis of eigenvectors. But all the eigenvalues of $T$ must be zero, so $T$ is zero on a basis for $V$ and is therefore zero.

Conversely, suppose $A$ has no nonzero nilpotents. Then $A$ is isomorphic to a product of finite extensions of $K$, and since $K$ is algebraically closed, this means that we have an isomorphism:

$$f : A \cong \prod_i K.$$

Let $e_i$ be an element of $A$ that maps to 1 in the $i$th copy of $K$ and zero in all the other factors. If we have $d$ factors, then $e_1 + \cdots + e_d = 1$ in $A$. Moreover $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$.

Let $f_i : A \to K$ be defined by $f_i(a) = f(a)_i$, where $f(a)_i$ is the $i$th factor of $f(a)$. We then have $ae_i = f_i(a)e_i$ for all $a \in A$. It follows that $ae_i v = f_i(a)e_i v$ for all $v \in V$; that is, $e_i V$ is a simultaneous eigenspace for all $a \in A$. It thus suffices to show that the $e_i V$ span $V$. But $v = 1v = (e_1 + \cdots + e_d)v = e_1 v + \cdots + e_d v$ for all $v \in V$, so this is clear.

2. Let $F(z) = q\prod(1-q^n)^{24}$. Show that $\frac{d}{dz}\log F(z) = \frac{6i}{\pi}G_2(z)$, where $G_2$ is the weight 2 Eisenstein series from the previous example sheet. Deduce that $\log F(-\frac{1}{z}) - \log z^{12}F(z)$ is constant, and show that this constant is zero. Conclude that $F = \Delta$.

We have

$$\begin{aligned}\frac{d}{dz}\log F(z) &= \frac{d}{dz}\log q + 24\Sigma\frac{d}{dz}\log(1-q^n)\\ &= 2\pi i - 48\pi i\Sigma_{n=1}^{\infty}\frac{nq^n}{1-q^n}\\ &= 2\pi i - 48\pi i\Sigma_{n=1}^{\infty}n\Sigma_{m=1}^{\infty}q^{nm}\\ &= 2\pi i - 48\pi i\Sigma_{d=1}^{\infty}\sigma_d(d)q^d = \frac{6i}{\pi}G_2(z)\end{aligned}$$

We then have:

$$\begin{aligned}\frac{d}{dz}\log F(-\frac{1}{z}) &= \frac{1}{z^2}\frac{6i}{\pi}G_2(-\frac{1}{z}) = \frac{6i}{\pi}(G_2(z) - \frac{2\pi i}{z})\\ &= \frac{d}{dz}\log F(z) + \frac{12}{z} = \frac{d}{dz}\log(z^{12}F(z)).\end{aligned}$$

So $\log F(-\frac{1}{z}) - \log z^{12}F(z)$ is constant, and so $F(-\frac{1}{z}) = cz^{12}F(z)$ for some constant $c$. Considering $z = i$ shows this constant is one, so $F$ is modular of weight 12 and thus a scalar multiple of $\Delta$. Comparing constant terms gives that $F = \Delta$.

3. Let $M_k(\mathbb{Z})$ be the space of modular forms of weight $k$ with integral $q$-expansions. Show that the graded ring:

$$\bigoplus M_k(\mathbb{Z})$$

is generated over $\mathbb{Z}$ by $E_4$, $E_6$, and $\Delta$.

This follows easily from the argument of problem 3 of example sheet 2; indeed, the $f_i$ constructed there are easily seen by induction to be integer polynomials in $E_4$, $E_6$, and $\Delta$, and any modular form with integral coefficients is an integral linear combination of the $f_i$.

4. Let $V$ be a *three* dimensional real vector space, and let $X$ be the set of lattices $L$ in $V$. For $(a, b)$ positive integers with $a$ dividing $b$, define a correspondence $T_{(a,b)} : \mathbb{Z}[X] \to \mathbb{Z}[X]$ that sends $L$ to the sum of $L' \subset L$ such that $L/L'$ is isomorphic to $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

4a. Show that if $(b, b') = 1$, then $T_{(a,b)}T_{(a',b')} = T_{(aa',bb')}$.

Notation: say $L' \subseteq_{a,b} L$ if $L'$ is a sublattice of $L$ such that $L/L'$ is isomorphic to $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Note that (for arbitrary $(a, b), (a', b')$) we have

$$T_{(a,b)})T_{(a',b')} = T_{(a,b)}\Sigma_{L' \subseteq_{a',b'} L}L' = \Sigma_{L' \subseteq_{a',b'} L}\Sigma_{L'' \subseteq_{a,b} L'}L''.$$

The latter sum can also be written as

$$\Sigma_{L''}c_{(a,b),(a',b')}(L'', L)L'',$$

where $c_{(a,b),(a',b')}(L'', L)$ is the number of lattices $L'$ such that $L'' \subseteq_{(a,b)} L' \subseteq_{(a',b')} L$. Note that the map $L' \mapsto L'/L''$ induces a bijection between the set of such $L'$ and the set of subgroups $A$ of $L/L''$ such that $A$ is isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$ and such that $(L/L'')/A$ is isomorphic to $\mathbb{Z}/a' \times \mathbb{Z}/b'$.

If we assume $b$ and $b'$ are relatively prime, then $a$ and $a'$ are as well. We will show that $c_{(a,b),(a',b')}L'' = 1$ if $L'' \subseteq_{(aa',bb')} L$ and zero otherwise.

First suppose that there exists an $L'$ such that such that $L'' \subseteq_{(a,b)} L' \subseteq_{(a',b')} L$. Then $L'/L''$ is a subgroup of $L/L''$ isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$ and the quotient by this subgroup is isomorphic to $L/L'$ and thus to $\mathbb{Z}/a \times \mathbb{Z}/b$. On the other hand, if $A$ is a finite abelian group, and $B$ is a subgroup of $A$ such that the orders of $B$ and $A/B$ are relatively prime, then $A$ is isomorphic to $B \times A/B$. (This follows from the fact that a finite abelian group is a product of its p-Sylow subgroups.) In this case that means that $L/L''$ is isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b \times \mathbb{Z}/a' \times \mathbb{Z}/b'$, which is isomorphic to $\mathbb{Z}/aa' \times \mathbb{Z}/bb'$ by the Chinese Remainder Theorem.

For such $L''$, $c_{(a,b),(a',b')}$ is equal to the number of subgroups of $\mathbb{Z}/aa' \times /\mathbb{Z}/bb'$ isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$ (the quotient by any such subgroup will be isomorphic to $\mathbb{Z}/a' \times \mathbb{Z}/b'$). It is easy to see there is exactly one such subgroup- namely the subgroup consisting of all elements whose order divides $b$.

Thus $T_{(a,b)}T_{(a',b')}L = \Sigma_{L'' \subseteq_{(aa',bb')} L}L'' = T_{(aa',b'')}L$.

4b. Fix a prime $p$, and express $T_{(1,p^2)}, T_{(1,p^3)}$, and $T_{(p,p^2)}$ as polynomials in $T_{(1,p)}, T_{(p,p)}$ and the "rescaling by $p$" operator $R_p$.

We have $T_{(1,p)}^2 L = \Sigma_{L''} c_{(1,p),(1,p)}(L'', L)L''$. If we have a lattice $L'$ such that $L'' \subseteq_{(1,p)} L' \subseteq_{(1,p)} L$, then $L''$ has index $p^2$ in $L$, so $L/L''$ is isomorphic either to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$. The former has exactly one cyclic subgroup of order $p$ (so $c_{(1,p),(1,p)}(L'', L) = 1$ in this case); the latter has $p+1$. Thus $T_{(1,p)}^2 L = T_{(1,p^2)}L + (p+1)T_{(p,p)}L$. This gives us $T_{(1,p^2)} = T_{(1,p)}^2 - (p+1)T_{(p,p)}$.

Next consider $T_{(1,p)}T_{(p,p)} = \Sigma_{L''} c_{(1,p),(p,p)}(L'', L)L''$. If $L'' \subseteq_{(1,p)} L' \subseteq_{(p,p)} L$, then $L''$ has index $p^3$ in $L$, so $L/L''$ is isomorphic to one of $ZZ/p^3$, $\mathbb{Z}/p^2 \times \mathbb{Z}/p$, or $(\mathbb{Z}/p)^3$. In fact, $L/L''$ cannot be cyclic as it has a quotient $L/L'$ that is isomorphic to $\mathbb{Z}/p^2$. Suppose $L/L''$ is isomorphic to $\mathbb{Z}/p^2 \times \mathbb{Z}/p$. Then $L/L''$ has exactly one cyclic subgroup $A$ such that $(L/L'')/A$ is isomorphic to $(\mathbb{Z}/p)^2$, namely the subgroup $p\mathbb{Z}/p^2 \times \{0\}$. Thus $c_{(1,p),(p,p)}(L'', L) = 1$ in this case. When $L/L''$ is isomorphic to $(\mathbb{Z}/p)^3$, then $L'' = pL$, and $L/L''$ has $p^2 + p + 1$ cyclic subgroups $A$ of order $p$. For any such, the quotient by $A$ is isomorphic to $(\mathbb{Z}/p)^2$. We thus have $c_{(1,p),(p,p)}(pL, L) = p^2 + p + 1$. It follows that $T_{(1,p)}T_{(p,p)} = T_{(p,p^2)} + (p^2 + p + 1)R_p$.

Now consider $T_{(1,p)}T_{(1,p^2)}$. If $L'' \subseteq_{(1,p)} L' \subseteq_{(1,p^2)} L$, then $L''$ has index $p^3$ in $L$, and $L/L''$ cannot be isomorphic to $(\mathbb{Z}/p)^3$ since it has a quotient $L/L'$ that is cyclic of order $p^2$. Thus $L/L''$ is either $\mathbb{Z}/p^3$ (in which case $c_{(1,p),(1,p^2)}(L'', L) = 1$) or $\mathbb{Z}/p^2 \times \mathbb{Z}/p$. In the latter case $c_{(1,p),(1,p^2)}(L'', L)$ is equal to the number of cyclic subgroups of order $p$ in $L/L''$ such that the quotient is isomorphic to $\mathbb{Z}/p^2$. There are $p+1$ cyclic subgroups of order $p$ in $\mathbb{Z}/p^2 \times \mathbb{Z}/p$, and we saw in the last computation that for exactly one of these, the quotient was isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$. Thus in all other cases the quotient is isomorphic to $\mathbb{Z}/p^2$ and $c_{(1,p),(1,p^2)}(L'', L) = p$. It follows that $T_{(1,p)}T_{(1,p^2)} = T_{(1,p^3)} + pT_{(p,p^2)}$.

This yields:

$$T_{(1,p^2)} = T_{(1,p)}^2 - (p+1)T_{(p,p)}.$$

$$T_{(p,p^2)} = T_{(1,p)}T_{(p,p)} - (p^2 + p + 1)R_p.$$

$$T_{(1,p^3)} = T_{(1,p)}T_{(1,p^2)} - pT_{(p,p^2)} = T_{(1,p)}^3 - (p+1)T_{(1,p)}T_{(p,p)} - pT_{(1,p)}T_{(p,p)} + p(p^2+p+1)R_p.$$

In fact, any $T_{(a,b)}$ is a polynomial in the operators $T_{(1,p)}, T_{(p,p)}, R_p$ as $p$ runs over all the primes. Moreover, once can check that these operators all commute with each other!