**Jyväskylä Summer School 2006**

**Course MA2: Solutions to exercises**

Here you will find solutions to all the exercises I set during the course MA2, together with some I didn't have time to set during the lectures. I have retained the original numbering, although in the lecture notes provided by Tuomas Puurtinen for courses MA1 and MA2 my sections are numbers 2, 5, 6, 8, 9, 11, 12 and 14, with a corrresponding renumbering of exercises. If you have any questions about these solutions, please contact me at G.A.Jones@maths.soton.ac.uk. Gareth Jones

**Exercise 1.1.** Find the discriminant of the elliptic curve $y^2 = x^3 - 9x^2 + 23x - 15$. Put the curve into Weierstrass and Legendre normal forms.

**Solution.** $x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-5)$ has roots $e_j = 1, 3, 5$, so $\Delta = 16\prod_{j<k}(e_j - e_k)^2 = 2^{12} = 4096$.

Replacing $x$ with $ax + b$ converts the right-hand side of the equation into

$$\begin{aligned}&(ax+b)^3 - 9(ax+b)^2 + 23(ax+b) - 15\\ &= a^3x^3 + (3a^2b - 9a^2)x^2 + (3ab^2 - 18ab + 23a)x + (b^3 - 9b^2 + 23b - 15),\end{aligned}$$

so take $b = 3$ to removee the quadratic term and $a = 4^{1/3}$ to give a leading coefficient equal to 4. The resulting Weierstrass form is

$$y^2 = 4x^3 - 4^{4/3}x$$

with $g_2 = 4^{4/3}$ and $g_3 = 0$. Alternatively, replace $x$ with $x + 3$ to give $y^2 = x^3 - 4x$, and then replace $y$ with $y/2$ to give $y^2 = 4x^2 - 16x$. (The Weierstrass form is not unique.)

Replacing $x$ with $2x + 1$ converts the right-hand side into $2x(2x-2)(2x-4) = 8x(x-1)(x-2)$, and replacing $y$ with $2\sqrt{2}y$ converts the left-hand side into $8y^2$, giving Legendre form $y^2 = x(x-1)(x-2)$, with $\lambda = 2$. (Other solutions are possible, with $\lambda = 1/2$ or $-1$, depending on the affine transformation applied to $x$.)

**Exercise 1.2.** Show that $\wp'$ is doubly periodic wth respect to $\Lambda$, so that $\wp' \in F(\Lambda)$. Deduce that $\wp$ is doubly periodic wth respect to $\Lambda$, so that $\wp \in F(\Lambda)$.

**Solution.** As the derivative of a meromorphic function $\wp$, $\wp'$ is also meromorphic. Now

$$\wp(z)' = -2\sum_{\omega}(z-\omega)^{-3},$$

so if $\omega_j$ $(j = 1, 2)$ is one of the basis elements of $\Lambda$ then

$$\wp'(z+\omega_j) = -2\sum_{\omega}(z+\omega_j-\omega)^{-3} = -2\sum_{\omega}(z-(\omega-\omega_j))^{-3}.$$

Since $\Lambda$ is a group, and $\omega_j \in \Lambda$, it follows that as $\omega$ ranges over $\Lambda$ so does $\omega - \omega_j$. Thus the series for $\wp'(z+\omega_j)$ is simply a rearrangement of the series for $\wp(z)$, so (assuming absolute

convergence) we have $\wp'(z+\omega_j) = \wp'(z)$ for all $z$. Thus $\wp'$ is invariant under $\omega_1$ and $\omega_2$, and hence under $\Lambda$ since these basis elements generate $\Lambda$. This shows that $\wp' \in F(\Lambda)$.

Integrating $\wp'(z+\omega_j) = \wp'(z)$ with respect to $z$ gives $\wp(z+\omega_j) = \wp(z) + c_j$ for some constant $c_j$. Taking $z = -\omega_j/2$ we get $\wp(-\omega_j/2) = \wp(\omega_j/2) + c_j$, finite since $\wp$ is holomorphic on $\mathbf{C} \setminus \Lambda$. By inspection of its defining series, $\wp$ is an even function (since $-\Lambda = \Lambda$), so $\wp(-\omega_j/2) = \wp(\omega_j/2)$ and hence $c_j = 0$. Thus $\wp(z+\omega_j) = \wp(z)$ for all $z$ and for $j = 1, 2$, so $\wp \in F(\Lambda)$.

**Exercise 1.3.** Show that $\Gamma$ acts transitively on the rational projective line $\hat{\mathbf{Q}} = P^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. Show that $\Gamma(2)$ has three orbits on $\hat{\mathbf{Q}}$, and deduce that $\Gamma/\Gamma(2)$ is isomorphic to $S_3$, the symmetric group of degree 3.

**Solution.** The group $\Gamma$ leaves $\hat{\mathbf{Q}}$ invariant, since if $\tau \in \hat{\mathbf{Q}}$ then $T(\tau) \in \hat{\mathbf{Q}}$ for each $T \in \Gamma$. Every rational number $r$ can be written in the form $a/c$ with $a$ and $c$ coprime integers. Then there exist integers $b$ and $d$ such that $ad - bc = 1$, and the corresponding transformation $T : \tau \mapsto (a\tau + b)/(c\tau + d)$ sends $\infty$ to $a/c = r$. Thus every element of $\mathbf{Q}$ is in the same orbit as $\infty$, so $\Gamma$ acts transitively on $\hat{\mathbf{Q}}$.

The elements $T$ of $\Gamma$ in $\Gamma(2)$ are those with $a$ and $d$ odd, $b$ and $c$ even. I claim that the orbits $[0], [1]$ and $[\infty]$ containing $0, 1$ and $\infty$ are the subsets of $\hat{\mathbf{Q}}$ consisting of those elements $r = p/q$ ($p$ and $q$ coprime integers) such that $p$ is even and $q$ is odd, $p$ and $q$ are both odd, and $p$ is odd and $q$ is even. (We write $\infty = 1/0$ here.) Then $T(r) = (ap + bq)/(cp + dq)$ with numerator and denominator having the same parity as $p$ and $q$, so these three subsets are invariant under $\Gamma(2)$. In the first paragraph, if $a$ is odd and $c$ is even, then $d$ is odd and we can choose $b$ to be even (replacing $b$ with $b' = b + a$ and $d$ with $d' = d + c$ if necessary, so that $ad' - b'c = 1$); thus $[\infty]$ is the orbit of $\Gamma(2)$ containing $\infty$. We can use similar arguments for the orbits $[0]$ and $[1]$, but the next part of the solution gives a quicker way.

Suppose that $r$ and $r'$ are in the same orbit of $\Gamma(2)$, say $r' = T(r)$ where $T \in \Gamma(2)$. If $S \in \Gamma$ then $S(r') = STS^{-1}(S(r))$ with $STS^{-1} \in \Gamma(2)$ since $\Gamma(2)$ is a normal subgroup of $\Gamma$, so $S(r)$ and $S(r')$ are in the same orbit of $\Gamma(2)$. Thus $\Gamma$ permutes the orbits of $\Gamma(2)$. (It now follows, by applying $X$ and $Z$ to $[0]$, that $[\infty]$ and $[1]$ are as described above.)

The action of $\Gamma$ on these three orbits gives a homomorphism $\theta : \Gamma \to S_3$. The generator $X : \tau \mapsto -1/\tau$ of $\Gamma$ transposes the orbits $[0]$ and $[\infty]$, and the generator $Y : \tau \mapsto (-\tau - 1)/\tau$ induces a 3-cycle $([0], [\infty], [1])$; these permutations generate $S_3$, so $\theta$ is an epimorphism. Since $\Gamma(2)$ leaves each of its orbits invariant it is contained in the kernel $\ker\theta$. But $\Gamma(2)$ and $\ker\theta$ both have index 6 in $\Gamma$, so they are equal. The first isomorphiasm theorem now gives $\Gamma/\Gamma(2) \cong S_3$.

**Exercise 1.4.** Evaluate $J$ at $\tau = i$ and at $\tau = \zeta_3$ ($= e^{2\pi i/3}$), and find the corresponding elliptic curves.

**Solution.** Firstly take $\tau = i$ and $\Lambda = \Lambda(1, i) = \{m + ni \mid m, n \in \mathbf{Z}\}$, the square lattice. Now $i\Lambda = \Lambda$, implying that as $\omega$ ranges over $\Lambda \setminus \{0\}$, so does $i\omega$. Thus $g_3 = 140 \sum'_\omega \omega^{-6} = 140 \sum'_\omega (i\omega)^{-6} = -140 \sum'_\omega \omega^{-6} = -g_3$, so $g_3 = 0$ and hence $J = g_2^3/(g_2^3 - 27g_3^2) = 1$. The elliptic curve $E$ corresponding to $\mathbf{C}/\Lambda$ has Weierstrass form $y^2 = 4x^3 - g_2x - g_3 = 4x^3 - g_2x$, and by multiplying $x$ and $y$ by suitable constants we can transform this into the isomorphic curve $y^2 = x(x^2 - 1)$, in Legendre form with $\lambda = -1$.

Secondly take $\tau = \zeta_3 = e^{2\pi i/3}$ and $\Lambda = \{m + n\zeta_3 \mid m, n \in \mathbf{Z}\}$, the hexagonal lattice. Then $\zeta_3\Lambda = \Lambda$, so a similar argument gives $g_2 = 60\sum'_\omega \omega^{-4} = 60\sum'_\omega(\zeta_3\omega)^{-4} = \zeta_3^{-1}g_2$. Thus $g_2 = 0$ and hence $J = 0$. The Weierstrass form is $y^2 = 4x^3 - g_3$, and as before, multiplying $x$ and $y$ by suitable constants, we can transform this to the simpler curve $y^2 = x^3 - 1$.

**Exercise 2.1.** If $x = (1, 2, \ldots, N)$ and $y = (1, 2)$ in $S_N$, draw the corresponding dessin $\mathcal{B}$ and find its monodromy group $G$.

**Solution.** The dessin $\mathcal{B}$ has a single black vertex $v$ of valency $N$, corresponding to the single cycle of $x$ of length $N$. If we number the edges $1, 2, \ldots, N$ in the positive order around $v$, then edges 1 and 2 meet at a single white vertex of valency 2, corresponding to the 2-cycle $(1, 2)$ in $y$, and each of the other $N - 2$ edges is incident with a white vertex of valency 1, corresponding to a fixed point of $y$. There are two faces, corresponding to the two cycles of $xy = (1)(2, 3, \ldots, N)$.

The monodromy group $G = \langle x, y\rangle$ is the symmetric group $S_N$: conjugating $y$ by powers of $x$ gives all transpositions of the form $(i, i + 1)$, and every cyclic permutation is a product of these, so every element of $S_N$ is a product of powers of $x$ and $y$.

**Exercise 2.2.** Show that $C \cong N_G(G_e)/G_e$ where $N(G_e)$ is the normaliser of $G_e$ in $G$.

**Solution.** Let $H = G_e$ for some fixed $e \in E$, and let $N = N_G(H)$. We will define an epimorphism $\alpha : N \to C$ with kernel $H$, so the first isomorphism theorem gives $N/H \cong C$. Each element of $E$ has the form $e' = eg$ for some $g \in G$, so let each $n \in N$ act on $E$ by sending $e'$ to $eng$. This is well-defined, since if $e' = eg_1 = eg_2$ then $g_1g_2^{-1} \in H$ so $ng_1g_2^{-1}n^{-1} \in H$ and hence $eng_1 = eng_2$. It is easy to check that $\alpha(n) : eg \mapsto eng$ is a permutation of $E$, and that it commutes with $G$, so $\alpha(n) \in C$. Now $\alpha(n_1n_2)$ sends $eg$ to $e(n_1n_2)g$, while (if we compose from right to left) $\alpha(n_1)\alpha(n_2)$ sends it via $en_2g$ to $en_1(n_2g)$, which is the same element of $E$; thus $\alpha$ is a homomorphism $N \to C$. (If we want to compose from left to right we need to define $\alpha(n) : eg \mapsto en^{-1}g$ to get a homomorphism.) If $n \in N$ then $n \in \ker\alpha$ if and only if $eng = eg$ for all $g \in G$, and this is equivalent to $en = e$, so $\ker\alpha = H$. To show that $\alpha$ is an epimorphism, let $c \in C$; then $ec = eg$ for some $g \in G$ by transitivity, and if $h \in H$ then $eghg^{-1} = echg^{-1} = ehcg^{-1} = ecg^{-1} = e$, so $ghg^{-1} \in H$ and hence $g \in N$; thus the elements $c$ and $\alpha(g)$ of $C$ both send $e$ to the same element, so $c = \alpha(g)$ since $C$ acts semiregularly.

**Exercise 2.3.** If $\mathcal{B}$ is a regular dessin of type $(l, m, n)$ with $N$ edges, what is its genus? Are there finitely or infinitely many regular dessns of a given type and genus?

**Solution.** Since $G$ acts regularly on $E$, all cycles of $x$ have the same length $l$, so there are $N/l$ of them, giving $N/l$ black vertices. Similarly, there are $N/m$ white vertices and $N/n$ faces. Since there are $N$ edges the Euler characteristic is

$$\chi = \frac{N}{l} + \frac{N}{m} - N + \frac{N}{n} = N\Big(\frac{1}{l} + \frac{1}{m} + \frac{1}{n} - 1\Big)$$

and so the genus is

$$g = 1 - \frac{\chi}{2} = 1 + \frac{N}{2}\Big(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\Big).$$

If $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}\neq 1$ then $l,m,n$ and $g$ determine $N$ uniquely. There are only finitely many groups $G$ of each order $N$, and each $G$ has only finitely many generating pairs $x,y$, so there are only finitely many corresponding regular dessins of type $(l,m,n)$ and genus $g$.

If $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}=1$, however, so that $g=1$, the value of $N$ is *not* uniquely determined, and this argument fails. This happens when $l,m$ and $n$ are permutations of $2,4,4$ or $2,3,6$ or $3,3,3$, and in each of these cases one can construct infinitely many regular dessins of type $(l,m,n)$ and genus $g=1$ by first constructing an infinite regular bipartite map of this type on $\mathbf{C}$, and then forming quotients by suitable lattices $\Lambda$. (The dessin $\mathcal{B}_3$ in Example 3, of type $(3,3,3)$, is an example of this construction, since one can extend the bipartite map to cover $\mathbf{C}$ by using copies of the basic hexagon as the tiles of a periodic tessellation.)

**Exercise 2.4.** Find $G, C, \tilde{\mathcal{B}}$ and $A$ if $\mathcal{B}$ is a path of $N$ edges, with vertices alternately black and white.

**Solution.** Successively number the edges $1,2,\ldots,N$. We may assume that the vertex incident with edge 1 is black (if not, transpose the colours). Then $x=(1)(2,3)(4,5)\ldots$, ending with $(N-1,N)$ or $(N-2,N-1)(N)$ as $N$ is odd or even, and $y=(1,2)(3,4)\ldots$, ending with $(N-2,N-1)(N)$ or $(N-1,N)$ respectively. These two permutations generate a dihedal group $D_N$ of order $2N$. One way to see this is by labelling the edges of a regular $N$-gon with $1,2,\ldots,N$ (not in cyclic order!) so that $x$ and $y$ induce reflections in axes subtending an angle $\pi/N$; these generate the symmetry group $D_N$ of the $N$-gon.

The stabiliser $G_1$ in $G$ of the edge 1 is the subgroup $\langle x\rangle\cong C_2$. If $N$ is odd then $N_G(G_1)=G_1$, so $C$ is the trivial group and $\mathcal{B}$ has no non-identity automorphisms. If $N$ is even then $N_G(G_1)$ is a Klein four-group generated by $x$ and the central involution $(xy)^{N/2}$, so $C$ has order 2; it is generated by $(xy)^{N/2}$, corresponding to the half-turn automorphism of $\mathcal{B}$.

The canonical regular cover $\tilde{\mathcal{B}}$ is the bipartite map corresponding to the regular representation of $D_N$. This is a circuit of $2N$ edges separating the sphere into two faces, with vertices alternately black and white. The subgroup $A\leq \operatorname{Aut}\tilde{\mathcal{B}}$, such that $\mathcal{B}\cong A\backslash\operatorname{Aut}\tilde{\mathcal{B}}$, is cyclic of order 2, generated by a half-turn of $\tilde{\mathcal{B}}$ about a black vertex. (This also fixes the antipodal vertex, coloured white or black as $N$ is odd or even.)

**Exercise 3.1.** Find the splitting field $K$ for the polynomial $f(x)=x^n-2\in\mathbf{Q}[x]$, describe $\operatorname{Gal}K/\mathbf{Q}$, and find the subgroups fixing $\zeta_n$ and $\alpha=2^{1/n}\in\mathbf{R}$.

**Solution.** The splitting field $K$ is generated by the roots $\alpha_k=\alpha\zeta_n^k$ of $f$, where $k=0,1,\ldots,n-1$. It therefore contains $\alpha=\alpha_0$ and $\zeta_n=\alpha_1/\alpha_0$. But these generate the roots $\alpha_k$, so $K=\mathbf{Q}(\alpha,\zeta_n)$.

The Galois group $G=\operatorname{Gal}K/\mathbf{Q}$ has order $|K:\mathbf{Q}|=|K:\mathbf{Q}(\zeta_n)|.|\mathbf{Q}(\zeta_n):\mathbf{Q}|=n\phi(n)$, and it permutes the roots $\alpha_k$ faithfully. Each $g\in G$ is uniquely determined by the images of $\zeta_n$, which must be a primitive $n$th root of unity $\zeta_n^j$ for some $j\in U_n$, and of $\alpha$, which must be a root $\alpha_k$ of $f$ for some $k\in\mathbf{Z}_n$, so we can write $g=g_{j,k}$. The elements $g_{1,k}$ fixing $\zeta_n$ form a normal subgroup $N$ of $G$, corresponding to the Galois extension $\mathbf{Q}(\zeta_n)$ of $\mathbf{Q}$; this is cyclic of order $n$ since $g_{1,k}\circ g_{1,k'}=g_{1,k+k'}$. The elements $g_{j,0}$ fixing $\alpha$ form a non-normal subgroup $H$ of $G$, corresponding to the non-Galois extension $\mathbf{Q}(\alpha)$ of $\mathbf{Q}$; this is isomorphic to $U_n$ since $g_{j,0}\circ g_{j',0}=g_{jj',0}$. The group $G$ is a semidirect product of $N$ by

$H$, isomorphic to the group of invertible affine transformations $z \mapsto jz+k$ ($j \in U_n, k \in \mathbf{Z}_n$) of $\mathbf{Z}_n$. (This is a generalisation of Example 3 in the Galois Theory lecture, which deals with the case $n = 3$.)

**Exercise 3.2.** Show that $\cup_{n\geq 1}\mathbf{Q}(\zeta_n)$ is a subfield of $\overline{\mathbf{Q}}$, and describe its Galois group.

**Solution.** Let $K$ denote $\cup_{n\geq 1}\mathbf{Q}(\zeta_n)$. The fields $\mathbf{Q}(\zeta_n)$ are all contained in $\overline{\mathbf{Q}}$, and hence so is their union $K$. If $\alpha, \beta \in K$ then $\alpha \in \mathbf{Q}(\zeta_l)$ and $\beta \in \mathbf{Q}(\zeta_m)$ for some $l$ and $m$, so $\alpha, \beta \in \mathbf{Q}(\zeta_n)$ where $n = \mathrm{lcm}(l, m)$; since $\mathbf{Q}(\zeta_n)$ is a field it contains $\alpha \pm \beta, \alpha\beta$ and $\alpha/\beta$ (if $\beta \neq 0$); it follows that these lie in $K$, which is therefore a field.

Whenever there is an inclusion $\mathbf{Q}(\zeta_n) \supseteq \mathbf{Q}(\zeta_m)$ (for instance when $m$ divides $n$), the field $\mathbf{Q}(\zeta_m)$ is invariant under $\mathrm{Gal}\,\mathbf{Q}(\zeta_n)/\mathbf{Q}$ since it is a Galois extension of $\mathbf{Q}$, so there is a restriction homomorphism $\rho_{n,m} : \mathrm{Gal}\,\mathbf{Q}(\zeta_n)/\mathbf{Q} \to \mathrm{Gal}\,\mathbf{Q}(\zeta_m)/\mathbf{Q}$. By an argument similar to that applied to $\mathbf{G}$ in the lectures, $\mathrm{Gal}\,K/\mathbf{Q}$ can be identified with the projective limit $\lim_{\leftarrow} \mathrm{Gal}\,\mathbf{Q}(\zeta_n)/\mathbf{Q}$ of these groups and homomorphisms, that is, with the group

$$\{(g_n) \in \prod_n \mathrm{Gal}\,\mathbf{Q}(\zeta_n)/\mathbf{Q} \mid \rho_{n,m}(g_n) = g_m \text{ whenever } \mathbf{Q}(\zeta_n) \supseteq \mathbf{Q}(\zeta_m)\}$$

This is an abelian group, since $\mathrm{Gal}\,\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is isomorphic to the group $U_n$ of units mod $(n)$, and this is abelian. It is a quotient of $\mathbf{G}$ since $K$ is a Galois extension of $\mathbf{Q}$. (It is in fact the largest abelian quotient $\mathbf{G}^{\mathrm{ab}} = \mathbf{G}/\mathbf{G}'$ of $\mathbf{G}$, where $\mathbf{G}'$ denotes the commutator subgroup of $\mathbf{G}$; this depends on a deep theorem of Hilbert and Weber, that every finite Galois extension of $\mathbf{Q}$ with an abelian Galois group is contained in some cyclotomic field $\mathbf{Q}(\zeta_n)$.)

**Exercise 3.3.** What are the cardinalities of $\overline{\mathbf{Q}}$ and of $\mathbf{G}$?

**Solution.** $\overline{\mathbf{Q}}$ is infinite since it contains $\mathbf{Q}$. There are only countably many polynomials $f(x) = a_0 + \cdots + a_n x^n$ in $\mathbf{Q}[x]$ (finitely many for each value of $\sum_i |a_i| + n$ in $\mathbf{N}$), and each has only finitely many roots, so $\overline{\mathbf{Q}}$, as a union of countably many finite sets, is countable. Thus $|\overline{\mathbf{Q}}| = \aleph_0$.

To see that $\mathbf{G}$ is uncountable, consider a strictly ascending chain $\mathbf{Q} = K_1 \subset K_2 \subset \cdots$ of fields in $\mathcal{K}$, such as $K_n = \mathbf{Q}(\zeta_{2^n})$. For each $n$, the group $G_n = \mathrm{Gal}\,K_n/\mathbf{Q}$ is the quotient of $G_{n+1}$ by its normal subgroup $\mathrm{Gal}\,K_{n+1}/K_n$, which means that each $g_n \in G_n$ extends in $|\mathrm{Gal}\,K_{n+1}/K_n| = |K_{n+1} : K_n|$ ways to an element $g_{n+1} \in G_{n+1}$. As in Exercise 3.2, the field $K = \cup_{n\geq 1} K_n$ is a Galois extension of $\mathbf{Q}$, and its Galois group $\mathrm{Gal}\,K/\mathbf{Q}$ is the projective limit $\lim_{\leftarrow} G_n = \{(g_n) \in \prod_n G_n \mid \rho_{n,m}(g_n) = g_m \text{ whenever } n \geq m\}$ of the groups $G_n$ and the restriction homomorphisms $\rho_{n,m} : G_n \to G_m$ where $n \geq m$. There are $2^{\aleph_0}$ ways of extending $g_1$ to $g_2$, $g_2$ to $g_3$, and so on, so this Galois group has cardinality $2^{\aleph_0}$. Since it is an epimorphic image of $\mathbf{G}$, it follows that $\mathbf{G}$ has cardinality at least $2^{\aleph_0}$. As a product of countably many finite sets, $\Pi$ has cardinality at most $2^{\aleph_0}$, and hence so has its subgroup $\mathbf{G}$. Thus $|\mathbf{G}| = 2^{\aleph_0}$.

**Exercise 3.4.** Show that $\mathbf{G}$ is a closed subgroup of $\Pi$, and that $\Pi$ and $\mathbf{G}$ are compact Hausdorff spaces.

**Solution.** If $K \supseteq L$ in $\mathcal{K}$, then the discrete topologies on $G_K$ and $G_L$ induce the discrete topology on $G_K \times G_L$, so the set of pairs $(g_K, g_L)$ such that $\rho_{K,L}(g_K) \neq g_L$ is open in $G_K \times G_L$. It follows that its inverse image in $\Pi$ is open. This consists of all elements of $\Pi$ satisfying $\rho_{K,L}(g_K) \neq g_L$ for this particular pair $K$ and $L$, so the complement $C_{K,L}$ of this set, consisting of all elements of $\Pi$ satisfying $\rho_{K,L}(g_K) = g_L$, is closed. Now $\mathbf{G}$ is the intersection of these sets $C_{K,L}$ for all pairs $K \supseteq L$ in $\mathcal{K}$, so $\mathbf{G}$ is closed.

For each $K \in \mathcal{K}$ the group $G_K$ is finite and hence compact, so Tychonoff's Theorem implies that $\Pi$, as a product of compact spaces, is compact. If $g = (g_K)$ and $h = (h_K)$ are distinct elements of $\Pi$ then $g_k \neq h_K$ for some $K \in \mathcal{K}$; the sets $\{g_K\}$ and $\{h_K\}$ are open in $G_K$, so their inverse images in $\Pi$ are disjoint open sets containing $g$ and $h$. Thus $\Pi$ is a Hausdorff space. As a closed subset of a compact Hausdorff space, $\mathbf{G}$ is also compact and Hausdorff.

**Exercise 3.5.** Show that in any topological group, each open subgroup is closed, and each closed subgroup of finite index is open.

**Solution.** If $H$ is an open subgroup of a topological group $G$, then since multiplication is continuous, every coset $Hg$ of $H$ in $G$ is also open. Thus $G \setminus H$, a union of such cosets, is open and hence $H$ is closed. If $H$ is a closed subgroup of finite index in $G$, then $G \setminus H$, a union of finitely many closed cosets, is closed and hence $H$ is open. (This can fail for closed subgroups of infinite index: consider $\mathbf{Z}$ as a subgroup of the additive group $\mathbf{R}$, for instance.)

**Exercise 4.1.** Show that $\theta$ and $\phi$ (ingredients in a covering of bipartite maps) must be epimorphisms.

**Solution.** $\theta$ maps $x$ to $x'$ and $y$ to $y'$; since $x'$ and $y'$ generate $G'$, $\theta$ maps $G$ onto $G'$. Now let $e_0 \in E$ and let $e_0' = \phi(e_0) \in E'$. Any element $e' \in E'$ has the form $e' = e_0' g'$ for some $g' \in G'$, since $G'$ is transitive on $E'$. Since $\theta$ is onto, we have $g' = \theta(g)$ for some $g \in G$. Define $e = e_0 g$. Then $\phi(e) = \phi(e_0 g) = \phi(e_0)\theta(g) = e_0' g' = e'$, so $e' \in \phi(E)$. Thus $\phi$ maps $E$ onto $E'$.

**Exercise 4.2.** Explain Example 4 (that in the case of the Fermat curve, $\mathrm{Aut}\, X$ is a semidirect product of $\mathrm{Aut}\, \mathcal{B}$ by $S_3$) by giving a geometric description of $N_{PSL_2\mathbf{R}}(\Delta_e)$.

**Solution.** $\mathrm{Aut}\, \mathcal{B}$ is induced by the normal inclusion of $\Delta_e = \Delta'$ in the triangle group $\Delta = \Delta(n, n, n)$. The basic triangle $T$ for $\Delta$, with internal angles $\pi/n$, has a barycentric subdivision into six triangles $\tilde{T}$ with internal angles $\pi/2, \pi/3, \pi/2n$, and the corresponding triangle group $\tilde{\Delta} = \Delta(2, 3, 2n)$ contains $\Delta$. The index of $\Delta$ in $\tilde{\Delta}$ is equal to the ratio of the areas of their fundamental regions, and hence of the areas of $T$ and of $\tilde{T}$, namely 6. This is a normal inclusion, with $\tilde{\Delta}/\Delta \cong S_3$: for instance $\tilde{\Delta}$ permutes the three vertex colours in the triangulation of $\mathbf{H}$ associated with $\Delta$, inducing all 3! permutations, and $\Delta$ is the kernel of this action. The commutator subgroup $\Delta'$ is a characteristic subgroup of $\Delta$ (invariant under all automorphisms), so $\Delta_e = \Delta'$ is normal in $\tilde{\Delta}$. Thus $\tilde{\Delta}$ is contained in $N(\Delta_e)$ so $\tilde{\Delta}/\Delta_e$ acts as a group of automorphisms of the Riemann surface $X = \Delta_e \backslash \mathbf{H}$, with $\Delta/\Delta_e \cong \mathrm{Aut}\, \mathcal{B}$ as a normal subgroup of index 6. One can show that $N(\Delta_e) = \tilde{\Delta}$, so

that $\mathrm{Aut}\, X = \tilde{\Delta}/\Delta_e$, for instance by using areas of fundamental regions to show that $\tilde{\Delta}$ is a maximal Fuchsian group.

**Exercise 4.3.** Show that $\Delta[3,2,\infty] = PGL_2(\mathbf{Z})$, consisting of the transformations

$$\tau \mapsto \frac{a\tau + b}{c\tau + d} \quad \text{where } a,b,c,d \in \mathbf{Z},\ ad - bc = 1,$$

and

$$\tau \mapsto \frac{a\overline{\tau} + b}{c\overline{\tau} + d} \quad \text{where } a,b,c,d \in \mathbf{Z},\ ad - bc = -1.$$

**Solution.** The transformations $\tau \mapsto (a\tau + b)/(c\tau + d)$ with $a,b,c,d \in \mathbf{Z}$ and $ad - bc = -1$ transpose the upper and lower half planes, so if we compose them with complex conjugation we get isometries of $\mathbf{H}$, reversing orientation. The standard generators of $\Delta[3,2,\infty]$ are the reflections $\tau \mapsto -\overline{\tau}$, $\tau \mapsto -\overline{\tau} - 1$ and $\tau \mapsto 1/\overline{\tau}$ in the sides of a hyperbolic triangle $T$ with vertices at $\zeta_3, i$ and $\infty$. These are visibly elements of $PGL_2(\mathbf{Z})$, so $\Delta[3,2,\infty]$ is a subgroup of $PGL_2(\mathbf{Z})$. Products of pairs of these reflections give the generators $X, Y, Z$ of the modular group $PSL_2(\mathbf{Z})$, so $\Delta[3,2,\infty]$ contains $PSL_2(\mathbf{Z})$. This has index 2 in $PGL_2(\mathbf{Z})$, and $\Delta[3,2,\infty]$ contains elements of the other coset, so $\Delta[3,2,\infty]$ must be the whole of $PGL_2(\mathbf{Z})$.

**Exercise 4.4.** Draw $\mathcal{B}_\infty$.

**Solution.** The vertices are the points $p/q \in \mathbf{Q}$ with $q$ odd, coloured black or white as $p$ is even or odd. By regularity, the edges are the images under $\Gamma(2)$ of the edge from 0 to 1. A typical element $\tau \mapsto (a\tau + b)/(c\tau + d)$ of $\Gamma(2)$, with $a$ and $d$ odd, $b$ and $c$ even, sends 0 to $b/d$ and 1 to $(a+b)/(c+d)$. Now $b(c+d) - d(a+b) = bc - ad = -1$, so if vertices $p/q$ and $r/s$ are joined by an edge then $ps - qr = \pm 1$. Conversely, if vertices $p/q$ and $r/s$ satisfy $ps - qr = \pm 1$ then $p$ and $r$ have opposite parity (since $q$ and $s$ are both odd), so transposing these vertices if necessary we may assume that $p$ is even and $r$ is odd. Replacing $p$ and $q$ with $-p$ and $-q$ if necessary, we may also assumethat $ps - qr = -1$. Then $\tau \mapsto ((r-p)\tau + p)/((s-q)\tau + q)$ is an element of $\Gamma(2)$, and it sends 0 to $p/q$ and 1 to $r/s$, so these vertices are joined by an edge. Thus vertices $p/q$ and $r/s$ are joined by an edge (which is a hyperbolic line) if and only if $ps - qr = \pm 1$. For instance, the black vertex 0 is joined to white vertices $\pm 1, \pm 1/3, \pm 1/5, \ldots$.

**Exercise 5.1.** What are the analogues of the quasiplatonic surfaces for genus $g = 1$?

**Solution.** These are the compact Riemann surfaces $X$ uniformised by normal subgroups $K$ of finite index in euclidean triangle groups $\Delta$, acting on $\mathbf{C}$. Such a group $\Delta = \Delta(l,m,n)$ must satisfy $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$, so the only possible types (up to permutation) are $(2,4,4)$, $(2,3,6)$ and $(3,3,3)$. In each case, only the translations have infinite order, so $K$ must be contained in the translation subgroup of $\Delta$, which is a lattice $\Lambda$ of index $4, 6$ or $3$ in $\Delta$ respectively.

We can identify $\Delta(2,4,4)$ with the group of affine transformations $z \mapsto az + b$ of $\mathbf{C}$, where $a = \pm 1$ or $\pm i$, and $b \in \mathbf{Z}[i] = \{m + ni \mid m,n \in \mathbf{Z}\}$; this is a semidirect product

of a normal subgroup $\Lambda$ consisting of the translations, given by $a = 1$, and a complement $\Delta_0 \cong C_4$ fixing 0, given by $b = 0$. Any subgroup $K \leq \Lambda$ is normalised by $\Lambda$, since $\Lambda$ is abelian, so $K$ is normal in $\Delta$ if and only if it is invariant under conjugation by the generator $z \mapsto iz$ of $\Delta_0$, which acts on $\Lambda$ by rotation through $\pi/2$ about 0. This is equivalent to $K$ having a basis $\{m + ni, -n + mi\}$, so $K$ is a square lattice, similar to $\Lambda$, with $\tau = i$, and $X = \mathbf{C}/K$ is the corresponding square torus, or equivalently the elliptic curve $y^2 = x(x^2 - 1)$ (see Exercise 1.4).

The cases $\Delta(2, 3, 6)$ and $\Delta(3, 3, 3)$ are similar, with $b \in \mathbf{Z}[\zeta_6] = \mathbf{Z}[\zeta_3]$, and $a$ a power of $\zeta_6$ or $\zeta_3$ respectively. In each case we find that $K$ is a hexagonal lattice, with $\tau = \zeta_3$ (or equivalently $\tau = \zeta_6 = \zeta_3 + 1$), corresponding to the elliptic curve $y^2 = x^3 - 1$.

**Exercise 5.2.** Show that $\Delta(3, 2, 7)$ has a fundamental region of area $\pi/21$, and that this is the smallest for any triangle group acting on $\mathbf{H}$.

**Solution.** The Gauss-Bonnet Theorem states that a hyperbolic triangle with internal angles $\alpha, \beta, \gamma$ has area $\pi - \alpha - \beta - \gamma$. If $\frac{1}{l} + \frac{1}{n} + \frac{1}{n} < 1$ then by putting $\alpha = \pi/l$, $\beta = \pi/m$ and $\gamma = \pi/n$ we see that a fundamental triangle for $\Delta[l, m, n]$ has area $\pi(1 - \frac{1}{l} - \frac{1}{n} - \frac{1}{n})$. Two adjacent copies of $T$ form a fundamental region for $\Delta(l, m, n)$, and this has area $2\pi(1 - \frac{1}{l} - \frac{1}{n} - \frac{1}{n})$. Putting $l = 3$, $m = 2$ and $n = 7$ we get the value $\pi/21$ for $\Delta(3, 2, 7)$.

To see that the fundamental region for any other hyperbolic triangle group $\Delta(l, m, n)$ has area $A > \pi/21$, we may assume without loss of generality that $l \leq m \leq n$. If $l \geq 4$ then $A \geq 2\pi(1 - \frac{1}{4} - \frac{1}{4} - \frac{1}{4}) = \pi/2 > \pi/21$. If $l = 3$ then $n \geq 4$ (otherwise $l = m = n = 3$ and the group is euclidean, not hyperbolic), so $A \geq 2\pi(1 - \frac{1}{3} - \frac{1}{3} - \frac{1}{4}) = \pi/6 > \pi/21$. If $l = 2$ and $m \geq 4$ then $n \geq 5$ (otherwise $m = n = 4$ and the group is euclidean), so $A \geq 2\pi(1 - \frac{1}{2} - \frac{1}{4} - \frac{1}{5}) = \pi/10 > \pi/21$. If $l = 2$ and $m = 3$ then $n \geq 8$ (if $n \leq 6$ the group is euclidean or spherical), so $A \geq 2\pi(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{8}) = \pi/12 > \pi/21$. Triangle groups with $l = m = 2$ are spherical, so we have dealt with all the hyperbolic cases.

(A similar but longer argument shows that $\Delta(3, 2, 7)$ has a fundamental region of least area among all Fuchsian groups.)

**Exercise 5.3.** Prove that there is no Hurwitz group of genus 2.

**Solution.** Such a group $G$ would have order $84(g - 1) = 84 = 2^2.3.7$, so by Sylow's Theorems (for the prime $p = 7$) it would have $n_7$ Sylow 7-subgroups $S$ of order 7, where $n_7$ divides $|G|$ and $n_7 \equiv 1$ mod (7). The only solution is $n_7 = 1$, so $S$ is a normal subgroup of $G$. By composing the natural epimorphisms $\Delta \to G$ and $G \to G/S$ we get an epimorphism $\theta : \Delta \to G/S$, where $G/S$ has order $84/7 = 12$. Since 7 does not divide 12, $G/S$ has no elements of order 7, so $\theta(Z) = 1$. Since $X^3 = Y^2 = XYZ = 1$ in $\Delta$ it easily follows that $\theta(X) = \theta(Y) = 1$ also, so $\theta$ is not an epimorphism and $G$ cannot exist.

**Exercise 5.4.** How many regular bipartite maps of type $(5, 5, 5)$ have automorphism group $A_5$?

**Solution.** Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be conjugacy classes of elements of order 5 in $G = A_5$. There are two such classes, each with 12 elements, so there are $2^3 = 8$ possible choices for $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$. For each choice, we can use Proposition 5.3 (the character formula) to count

solutions of $xyz = 1$ in $G$ where $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$, and then summing over the eight choices we get the total number of triples $x, y, z$ of elements of order 5 in $G$ with $xyz = 1$.

For each choice of conjugacy classes,

$$\frac{|\mathcal{X}|.|\mathcal{Y}|.|\mathcal{Z}|}{|G|} = \frac{12^3}{60}.$$

If we sum the values of $\sum_\chi \chi(x)\chi(y)\chi(z)/\chi(1)$ over all eight choices, the first character $\chi$ contributes 8 (namely 1 for each choice), the second and third each contribute $(\lambda^3 + 3\lambda^2\mu + 3\lambda\mu^2 + \mu^3)/3 = (\lambda + \mu)^3/3 = 1/3$, the fourth contributes $-2$ (namely $(-1)^3/4$ for each choice), and the fifth contributes 0. It follows that the total number of triples is

$$\frac{12^3}{60}.\Big(8 + \frac{1}{3} + \frac{1}{3} - 2 + 0\Big) = 192.$$

Such a triple must generate either $G$ or a cyclic group $H \cong C_5$. There are six subgroups $H \cong C_5$ in $G$ (the Sylow 5-subgroups), each generated by $4.3 = 12$ triples, so 72 triples do not generate $G$. The remaining $192 - 72 = 120$ triples do, and since $|\mathrm{Aut}\, G| = |S_5| = 120$ they form a single orbit under automorphisms. It follows that $\Delta(5, 5, 5)$ has a single normal subgroup $K$ with quotient $A_5$, so we obtain a single regular bipartite map of type $(5, 5, 5)$ with $\mathrm{Aut}\, \mathcal{B} \cong A_5$. It is represented by

$$X \mapsto x = (1, 2, 3, 4, 5), \quad Y \mapsto y = (1, 3, 4, 2, 5), \quad Z \mapsto z = (1, 4, 2, 3, 5),$$

(all conjugate in $A_5$), and by Exercise 2.3 it has genus 13.

**Exercise 6.1.** Can you get a regular embedding of $K_7$ from the bipartite map representing the Fano plane $P^2(F_2)$ on the torus? Can you get two of them?

**Solution.** The bipartite map $\mathcal{B}$ of genus 1 representing the Fano plane has seven black vertices and seven white vertices, corresponding to the points and lines of the Fano plane, with edges representing incident point-line pairs. It is a quotient of the universal bipartite map of type $(3, 3, 3)$ by a torsion-free normal subgroup $K$ of index 21 in the triangle group $\Delta(3, 3, 3)$. There are seven hexagonal faces in $\mathcal{B}$, and the dual map (with a vertex in each face of $\mathcal{B}$, and edges between vertices in adjacent faces) is a regular embedding $\mathcal{M}$ of $K_7$ in a torus. This triangular map corresponds to the normal inclusion of $K$ in the triangle group $\Delta(6, 2, 3)$, which contains $\Delta(3, 3, 3)$ with index 2, with $\mathrm{Aut}\, \mathcal{M} \cong \Delta(6, 2, 3)/K \cong AGL_1(7)$.

The mirror image of $\mathcal{B}$ (corresponding to a second subgroup $K$ of index 21 in $\Delta(3, 3, 3)$) gives another regular embedding of $K_7$, the mirror image of $\mathcal{M}$, which is not isomorphic as an oriented map to $\mathcal{M}$. Since $K_7$ has $\phi(n-1)/e = \phi(6)/1 = 2$ regular embeddings, these are the only ones. They can be obtained as maps $\mathcal{M}(\alpha)$ by taking the vertex set to be the field $F_7$, and using the generator $\alpha = 3$ or 5 of the multiplicative group $F_7^* = F_7 \setminus \{0\}$ to define the rotation $v + 1$, $v + \alpha$, $v + \alpha^2$, $\ldots$, $v + \alpha^5$ of neighbours around each vertex $v$.