Some Hints and Solutions to Homework Problems

Homework 1.

1. *Prove Euclid I.6 : if two angles in a tiangle are equal to each other then the triangle is isosceles.*

Euclid argues this way. Let a triangle ABC has the angle BAC equal the angle BCA but $|AB| > |BC|$. Take D on AC such that $|AD| = |BC|$. Then the triangles ADC and CBA have equal areas by the side-angle-side proposition, which is absurd since ADC is strictly inside CBA.

2. *Suppose that the triangles ABC and DEF have $|AB| = |DE|$, $|AC| = |DF|$ and the angle ABC equal the angle DEF. Does this imply that the triangles are congruent?*

No. Fix the angle ABC and the length $|AB|$. Circles centered at A may intersect the ray BC at two different points C and C'. Then the triangles ABC and ABC' are not congruent since one of them is strictly inside the other.

1.10. $T_a \circ R = R \circ T_{-a}$. Respectively,

$$(T_a \circ R) \circ (T_b \circ R) = (T_a \circ R) \circ (R \circ T_{-b}) = T_a \circ (R \circ R) \circ T_{-b} = T_a \circ T_{-b} = T_{a-b}.$$

1.18. $g \cdot g = e$ is equivalent to $g^{-1} = g$. If this is true for any $g \in G$, then for any $a, b \in G$ we have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

2.14. *If a linear transfromation A is an isometry then $A^tA = I$.*

The formula $(u+v)^2 = u^2+2uv+v^2$ applied to the dot-product of vectors shows how to express the dot-product in terms of sums and lengths of vectors:

$$\langle u, v\rangle = \frac{1}{2}\left(\langle u+v, u+v\rangle - \langle u, u\rangle - \langle v, v\rangle\right) \text{ for any } u, v.$$

Since A preserves lengths of all vectors and $A(u+v) = Au + Av$ (due to lineariry of A), we conclude that A preserves dot-products: $\langle Au, Av\rangle = \langle u, v\rangle$ for any u and v. Therefore for any u, v

$$0 = \langle Au, Av\rangle - \langle u, v\rangle = \langle A^tAu, v\rangle - \langle Iu, v\rangle = \langle (A^tA - I)u, v\rangle.$$

Thus for any u the vector $(A^tA - I)u = \mathbf{0}$ since it is orthogonal to any v. This means that the matrix $A^tA - I = 0$.

Homework 2.

1.15. $g = ag$ implies $e = gg^{-1} = (ag)g^{-1} = a(gg^{-1}) = ae = a$.

1.16. $gh = gk$ implies $g^{-1}(gh) = g^{-1}(gk)$ implies $(g^{-1}g)h = (g^{-1}g)k$ implies $eh = ek$ implies $h = k$.

1.17. $e = fg$ implies $g^{-1} = eg^{-1} = (fg)g^{-1} = f(gg^{-1}) = fe = f$.

2.20a. For any vector x we have $T_u(x) = x + u$. Thus

$$\rho(T_u(x)) = \rho(x + u) = \rho(x) + \rho(u) = T_{\rho(u)}(\rho(x)).$$

2.26b. *Hint:* Any isometry on the plane is the composition of a translation with a rotation or reflection. A translation can be written as the composition of two reflections in two parallel lines perpendicular to the direction of the translation. Thus compositions of a translation with a reflection can be represented as the composition of three reflections. The composition of a translation T_u with a rotation ρ is in fact the rotation through the same angle about the fixed point defined by the equation $\rho(x) + u = x$.

Homework 3.

1. Prove that a group homomorphism f from a group G to a group H maps the identity element of G to the identity element of H and maps inverse elements to inverse elements.

Indeed, $f(a)e_H = f(a) = f(ae_G) = f(a)f(e_G)$ implies $e_H = f(e_G)$. Similarly, $e_H = f(e_G) = f(aa^{-1}) = f(a)f(a^{-1})$ implies $f(a)^{-1} = f(a^{-1})$.

3.7. The subgroup C_4 of rotations in the group D_4 of symmetries of the square is a cyclic group of order 4. It is not isomorphic to V_4 since any cyclic subgroup in V_4 has at most two elements.

3.15a. The cyclic group generated by the rotation through an angle α is infinite cyclic when α is incommensurable with 2π and is finite of order $n = 1, 2, 3, ...$ when $\alpha = 2\pi/n$.

3.15b. $SO(2)$ is not isomorphic to $\mathbf{Z}_n$ because $SO(2)$ is infinite, and it is not isomorphic to $\mathbf{Z}$ because $\mathbf{Z}$ contains no finite cyclic subgroups of order > 1.

3.18. A regular n-gon has n equal angles with the total sum $\pi(n-2)$. Thus each angle is $\pi(n-2)/n$ which is $60^\circ, 90^\circ, 108^\circ, 120^\circ, ...$ for $n = 3, 4, 5, 6, ...$ respectively.

The sum of face's angles at a vertex of a *convex* regular polyhedron is $< 360°$. Therefore the only possible configurations of such faces near a vertex are: three regular triangles, squares or pentagons, or four or five regular triangles.

Homework 4.

4.5bc. The "stereographic" projection of the circle $x^2 + y^2 = 1$ yields the description of integer Pythagorean triples $a^2 + b^2 = c^2$ in the form $a = r^2 - s^2$, $b = 2rs$, $c = r^2 + s^2$ where $r > s$ are integers. Thus an integer c is the hypotenuse of a right triangle with integer legs if and only if c can be written as the sum of squares of two distinct positive integers. For $c \le 13$, the available squares are $1, 4, 9$, and the required values of c are $5 = 1 + 4$, $10 = 1 + 9$ and $13 = 4 + 9$.

5.5+5.6. $p(x) := x^3 + 3x - 4$ is increasing since $p'(x) = 3x^2 + 3 > 0$. Therefore $p(x) = 0$ has at most one real solution, which obviously is $x = 1$. Thus the real solution $x = y - 1/y$ where $y := (2 + \sqrt{5})^{1/3}$ is in fact equal to 1. Therefore for $y > 0$ we have the quadratic equation $y^2 - y - 1 = 0$ and find $y = (1 + \sqrt{5})/2$. Thus $(2 + \sqrt{5})^{1/3} = (1 + \sqrt{5})/2$.

5.9. $x^3 + 3x - 4$ has a root $x = 1$ and is therefore divisible by $x - 1$. Explicitly we have $x^3 + 3x - 4 = (x - 1)(x^2 + x + 4)$. Thus the other two roots are solutions to $x^2 + x + 4 = 0$. These are $(-1 \pm i\sqrt{15})/2$.

Homework 5.

5.22. By definition, the point at ∞ plays the role of 0 in the group structure of the elliptic curve $E : y^2 + y = x^3 - x$. The symmetry $(x, y) \mapsto (x, -1 - y)$ about the line $y = -1/2$ (found by completing the square $y^2 + y = (y + 1/2)^2 - 1/4$) plays the role of taking the opposite $R \mapsto -R$ in the group E. The sum is defined by requiring that $P + Q + R = 0$ whenever $P, Q, R \in E$ are on the same line.

The line $x = t, y = 0$ passes through $P = (0, 0)$ and $Q = (1, 0)$ at $t = 0, 1$ and intersects E when $0 = t^3 - t$ which has solutions $t = 0, 1, -1$. Thus $P + Q + R = 0$ for $R = (-1, 0)$ and $S := P + Q = -R = (x, -1 - y) = (-1, -1)$.

Furthermore, the tangent line to E at $S = (x_0, y_0) = (-1, -1)$ is given by the equation $(2y_0 + 1)(y - y_0) = (3x_0^2 - 1)(x - x_0)$ i.e. $y = -2x - 3$ or $x = t, y = -2t - 3$. It intersects E when $(2t+3)^2 - (2t+3) = t^3 - t$ or, equivalently, $t^3 - 4t^2 - 11t - 6 = 0$. It has the double root at $t = -1$ (due to the tangency at S) and therefore has one more root $t = 6$. Thus the other root is $x = 6$, and $2S = -T = (t, -1 + 2t + 3)|_{t=6} = (6, 14)$.

Similarly, the line $x = -t, y = -t$ passes through P, S at $t = 0, 1$ and meets E when $t^2 - t = -t^3 + t$, at $t = 0, 1$ and therefore -2. Thus $S + P = (x, -1 - y) = (2, -3)$. The line $x = t + 1, y = -3t$ passes through $Q, S + P$ at $t = 0, 1$ and meets E when $9t^2 - 3t = t^3 + 3t^2 + 3t + 1 - t - 1$. The latter equation has solutions $t = 0, 1$ and therefore 5. Thus $(S + P) + Q = (x, -1 - y) = (5 + 1, -1 + 15) = (6, 14) = 2S$ (as expected!)

Finally, the line $x = 1 - 2t, y = -t$ passes through Q, S at $t = 0, 1$ and intersects E when $t^2 - t = -8t^3 + 12t^2 - 6t + 1 - 1 + 2t$ or, equivalently, $8t^3 - 11t^2 + 3t = t(t-1)(8t-3) = 0$ which has solutions $t = 0, 1$ and $3/8$. Thus $S + Q = (x, -1 - y) = (1/4, -5/8)$. The line $x = 2t, y = -5t$ passes through $P, S + Q$ at $t = 0, 1/8$ and meets E when $25t^2 - 5t = 8t^3 - 2t$, i.e. at $t = 0, 1/8$ and therefore 3. Thus $P + (S + Q) = (x, -1 - y) = (6, 14) = 2S$ — as expected!

5.25. $x^4+4x-1=0$ is equivalent to $(x^2+y)^2=2yx^2-4x+y^2+1$. The R.H.S. is a complete square if $16=8y(y^2+1)$ or, equivalently, $y^3+y-2=0$. This is satisfied for $y=1$. We have $(x^2+1)^2=2(x-1)^2$, or $x^2+1=\pm\sqrt{2}(x-1)$. Thus the roots are:

$$x_{1,2}=\frac{\sqrt{2}\pm i\sqrt{10+8\sqrt{2}}}{2},\quad x_{3,4}=\frac{-\sqrt{2}\pm\sqrt{8\sqrt{2}-10}}{2}.$$

6.22. If $\alpha^5=1$ then $|\alpha|=1$, hence $\bar{\alpha}=1/\alpha$ and therefore $Tr(\alpha)=\alpha+\alpha^{-1}$. If $\alpha\neq 1$ then $\alpha^4+\alpha^3+\alpha^2+\alpha+1=0$ or $\alpha^2+\alpha+1+\alpha^{-1}+\alpha^{-2}=0$. Putting $t:=\alpha+\alpha^{-1}$ we find $t^2=\alpha^2+2+\alpha^{-2}$ and conclude that $0=1+t+t^2-2=t^2+t-1$. Thus $t_\pm=(-1\pm\sqrt{5})/2$, and we have two quadratic equations $\alpha^2-t_\pm\alpha+1=0$ for the four roots $\alpha\neq 1$ of x^5-1. Thus

$$x^5-1=(x-1)\ (x^2+\frac{\sqrt{5}+1}{2}x+1)\ (x^2-\frac{\sqrt{5}-1}{2}x+1).$$

6.24b. $x^2-ix+1=0$ has solutions $x=(i\pm\sqrt{i^2-4})/2=(1\pm\sqrt{5})i/2$.

6.27. The norms $N=a^2+b^2<14$ of Gaussian integers $a+bi$ and the corresponding Gaussian integers are:
$N=0=0^2+0^2,\ a+bi=0$
$N=1=1^2+0^2,\ a+bi=\pm 1,\pm i,$
$N=2=1^2+1^2,\ a+bi=\pm 1\pm i,$
$N=4=2^2+0^2,\ a+bi=\pm 2,\pm 2i,$
$N=5=2^1+1^2,\ a+bi=\pm 2\pm i,\pm 1+\pm 2i,$
$N=8=2^2+2^2,\ a+bi=\pm 2\pm 2i,$
$N=9=3^2+0^2,\ a+bi=\pm 3,\pm 3i,$
$N=10=3^2+1^2,\ a+bi=\pm 3\pm i,\pm 1\pm 3i,$
$N=13=3^2+2^2,\ a+bi=\pm 3\pm 2i,\pm 2\pm 3i.$

Homework 6.

1. On the elliptic curve $y^2 = (x-1)(x-2)(x-3)$, find all points P which satisfy the condition $P + P = 0$ with respect to the group law $+$ on the curve. Show that these points form a subgroup isomorphic to the Klein group V_4.

These are points fixed under the symmetry $P \mapsto -P$ defined as $(x, y) \mapsto (x, -y)$ and thus correspond to $y = 0$. There are four such points: the zero element at infinity and the three finite symmeric points P_1, P_2, P_3 defined by $(x, y) = (1, 0), (2, 0), (3, 0)$. They are on the same line $y = 0$ and thus $P_1 + P_2 + P_3 = 0$. This $P_1 + P_2 = P_3$, etc. so that the four points form a subgroup. An isomorphism with the symmetry group V_4 of a rectangle is established by sending P_1 and P_2 to the reflections of the rectangle about its symmetry lines and sending P_3 to their product — the central symmetry.

2. Use the algorithm from the proof of the Newton-Waring theorem to express $r^4 + s^4 + t^4 + u^4$ as a polynomial in the elementary symmetric functions of the four variables r, s, t, u.

$$r^4 + s^4 + t^4 + u^4 = s_1^4 - 4(r^3 s + ...) - 6(r^2 s^2 + ...) - 12(r^2 st + ...) - 24rstu$$
$$= s_1^4 - 4s_1^2 s_2 + (8-6)(r^2 s^2 + ...) + (20-12)(r^2 st + ...) + (48-24)rstu$$
$$= s_1^4 - 4s_1^2 s_2 + 2s_2^2 + (20-12-4)(r^2 st + ...) + (48-24-12)rstu$$
$$= s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3 + (48-24-12-16)rstu$$
$$= s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3 - 4s_4.$$

7ab. By the fundamental theorem of algebra a complex polynomial factors as $(z - z_1)...(z - z_n)$ where z_i are complex roots. A polynomial with real coefficients is invariant under the complex conjugation and thus has an invariant set of roots and their multiplicities. Thus each root is either real or comes in a complex conjugate pair. In the latter case the product of the factors $(z-a)(z-\bar{a}) = z^2 - Tr(a)z + N(a)$ has real coeffcieients. In particular, irreducible polynomials in $\mathbf{R}[x]$ are either linear or quadratic with negative discriminant.

7c. $x^2 - 2$ and $x^3 - 2$ factor in $\mathbf{R}[x]$ but are irreducible in $\mathbf{Q}[x]$. Indeed, if reducible, they would have a linear factor and thus a root in $\mathbf{Q}$, which they don't.

Homework 7.

7.8. Permitations of $1,2,3$ also permute the pairs $(1,2),(1,3),(2,3)$ and thus permute the factors $(r_i - r_j)$ in the product δ (but possibly reverse their signs). Thus $\sigma(\delta) = \pm\delta$.

7.9. One way to check that $\delta^2(r_1,r_2,r_3) = 4p^3 - 27q^2$, where r_i are the roots of the polynomial $x^3 - px + q$, is to substitute $\delta = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3) = (r_1 - r_2)(2r_1 + r_2)(r_1 + 2r_2)$ on the left and $p = -(r_1 + r_2)r_3 - r_1r_2 = r_1^2 + r_1r_2 + r_2^2$ and $q = -r_1r_2r_3 = r_1^2r_2 + r_1r_2^2$ on the right.

7.12. If $\bar{f} = \sum_{h\in H} h(f)$ then for any $\sigma \in H$

$$\sigma(\bar{f}) = \sum_{h\in H}(\sigma h)f = \sum_{\sigma^{-1}g\in H} g(f) = \sum_{g\in H} g(f) = \bar{f}.$$

7.13. To prove Mathieu's theorem, put $p(r_1,...,r_n) = r_1^{n-1}r_2^{n-2}...r_{n-1}^1 r_n^0$. Then for all $\sigma \in S_n$ the monomials $\sigma(p) = r_{\sigma(1)}^{n-1}...r_{\sigma(n)}^0$ are distinct (and hence linearly independent). For a given subgroup $H \in S_n$ put $f = \bar{p} = \sum_{h\in H} h(p)$. If $\sigma \notin H$ then $\sigma(f) \neq f$ since it contains the monomial $\sigma(p)$ which is not present in f. If $\sigma \in H$ then $\sigma(f) = f$ by 7.12. Thus $(S_n)_f = H$.

7.10c is a special case of 7.13 with $n = 3$.

Homework 8.

8.1. Cycle structures of permutations from S_n correspond to *partitions* n (i.e. $4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$). Permutation with a given cycle structure correcponding to a partition P with m_1 ones, m_2 twos, m_2 threes, etc. are obtained by fitting $1,2,3,...,n$ (where $n = m_1 + 2m_2 + 3m_3 + ...$) in any order into the format of m_1 cycles of length 1, m_2 cycles of length 2, etc. Yet two fittings yield the same permutation if they are obtained from each other by cyclic shifts within the cycles and/or by permuting the m_k cycles of the same length $k = 1,2,3,....$ Thus the total number of permutations of $1,2,...,n$ with a given cycle structure is equal to

$$\#(P) = \frac{n!}{1^{m_1}(m_1)!\ 2^{m_2}(m_2)!\ 3^{m_3}(m_3)!\ \cdots}$$

In the example of $n = 4$ we have:

$$P = 4, \# = 24/4 : (1234), (1324), (2134), (2314), (3124), (3214)$$

$$P = 3 + 1, \# = 24/3 : (123), (213), (124), (214), (134), (314), (234), (324)$$

$$P = 2 + 2, \# = 24/8 : (12)(34), (13)(24), (14)(23)$$

$$P = 2 + 1 + 1, \# = 24/4 : (12), (13), (14), (23), (24), (34)$$

$$P = 1 + 1 + 1 + 1, \# = 24/24 : \text{ the identity permutation.}$$

8.7. There are 3 ways to partition $\{1, 2, 3, 4\}$ into two pairs: $\{12\}\{34\}$, $\{13\}\{24\}$, $\{14\}\{23\}$. Respectively, the S_4-orbit of $G = (r_1+r_2)(r_3+r_4)$ consists of 3 elements:

$$G,\ G' = (r_1 + r_3)(r_2 + r_4),\ G'' = (r_1 + r_4)(r_2 + r_3).$$

Thus $(X - G)(X - G')(X - G'') = X^3 + AX^2 + BX + C$, where A, B, C are polynomials of elementary symmetric functions in r_1, r_2, r_3, r_4. Assuming that r_i's are roots of $x^4 + cx^2 + dx + e$ (and therefore $r_1 + r_2 + r_3 + r_4 = 0$), we find $G = -(r_1+r_2)^2$ and similarly $G' = -(r_1+r_3)^2$, $G'' = -(r_1+r_4)^2$. Thus the equation $x^4+cx^2+dx+e = 0$ can be solved as follows. First, compute A, B, C as polynomials in the elementary symmetric functions $c, -d, e$. Next find G, G', G'' as roots of the cubic equation $X^3 + AX^2 + BX + C = 0$. Then compute $r_1 + r_2, r_1 + r_3, r_1 + r_4$ as square roots of $-G, -G', -G''$. Finally solve these linear equations (together with $r_1 + r_2 + r_3 + r_4 = 0$) for r_1, r_2, r_3, r_4.

8.6a. Similarly to the case of G, the orbit of F consists of 6 elements

$$\pm F = \pm(r_1 - r_2)(r_3 - r_4),\ \pm F' = \pm(r_1 - r_3)(r_2 - r_4),\ \pm F'' = \pm(r_1 - r_4)(r_2 - r_3).$$

8.10. Let a group G acts by permutations on a set S, and let $H = G_a$ be the stabiliser of $a \in S$. For any b in the orbit $\mathcal{O}$ of a, the elements of the group G mapping a to b have the form gh where g is any particular element with this property, and h is any element from the stabilizer of a. Thus the number of the elements of G mapping a to b does not depend on $b \in \mathcal{O}$ and is equal to the number of elements $|H|$. Thus we have $|G| = |H| \times |\mathcal{O}|$.

Homework 9.

9.8 cde. The characteristic polynomial $det(\lambda I - T) = \lambda^3 + a\lambda^2 + b\lambda + c$ has odd degree and thus has a real root λ_0. Thus there exists $x_0 \in \mathbf{R}^3$, $|x_0| = 1$, such that $Tx_0 = \lambda_0 x_0$. Since $|Tx_0| = |x_0|$, we have $\lambda_0 = \pm 1$. If $\lambda_0 = -1$, then the other two roots have to be 1 and -1 since the product of all 3 roots equals $det(T) = 1$. (If the other two roots were complex conjugate, their product would've been positive, and the product of all 3 roots - negative). Thus in either case there is a unit eigenvector v with the eigenvalue 1. Since T preserves inner products and preserves the line spanned by v, T preserves the plane orthogonal to v and acts on it as an orthogonal transfromation with the determinant 1. Thus picking any orthonormal basis in this plane in the role of u and w, we find that T has in the basis v, u, w the required matrix.

9.9. Axis of rotation of a (non-identity) rotation S is the eigen-space corresponding to the eigenvalue 1. To show that $RS = SR$ implies that R fixes the rotation axis of S, we prove a more general statement: *any eigen-space of a linear operator S is invariant under any operator R commuting with S.* Indeed, if $Sx = \lambda x$ then $y := Rx$ also satisfies $Sy = SRx = RSx = \lambda Rx = \lambda y$.

9.15. The rotation group G of the cube acts on the set vertices of the cube and acts *transitively*, i.e. all the 8 vertices form one orbit. The stabilizer G_v of one vertex v consists of the 3 rotations (through the angles 0 and $\pm 2\pi i/3$) about the diagonal containing v. Thus $|G| = 8 \times 3 = 24$. Next, there is a homomorphism $\phi : G \to S_4$ defined by the action of G on the set of the 4 diagonals by permutations. To prove that ϕ is an isomorphism, observe that each of the 3 types of non-indetity rotations in G permutes some diagonals in a non-trivial way. Thus the kernel $ker(\phi) := \phi^{-1}(e) \subset G$ contains only the identity transformation. This implies that ϕ is injective, and since $|S_4| = 24$, it is surjective as well.

Homework 10.

1. Show that the rotation group of the dodecahedron is isomorphic to the group A_5 of all even permutations of 5 symbols (it is called the *alternating subgroup* in S_5). Hint: the rotations permute 5 cubes formed by the diagonals in the pentagonal faces of the dodecahedron (each cube having one edge in each of the 12 faces of the dodecahedron).

Outline. The hint describes the construction of a homomorphism $f : G \to S_5$ from the rotation group of the dodecahedron to the permutation group. We have $|G| = (\#\text{ of faces}) \times (\#\text{ of rotations preserving a face}) = 12 \times 5 = 60$ and $|A_5| = |S_5|/2 = 120/2 = 60$. It suffices therefore to prove that $f^{-1}(e) = \{e\}$ (injectivity) and that $f(G) \subset A_5$. The group G consists of the identity element and rotations through the angles $2\pi/5$ (about the axes passing through the centers of faces), $2\pi/3$ (about the axes passing through vertices) and $2\pi/2$ (about the axes passing through the midpoints of edges). Since G acts transitively on the sets of faces, vertices and edges, it suffices to consider only one rotation of each kind and check that it induces a non-trivial even permutation of the 5 cubes.

2. Find the greatest common divisor of 50339 and 128243.

The Euclidean algorithm shows in a few steps that the numbers are relatively prime, while an attempt to use prime factorization will require trying all prime factors up to 71 since $128243 = 257 \times 499$ and $50339 = 71 \times 709$ (in fact it was meant to be $50399 = 101 \times 499$ which would make the answer more interesting).

3. Referring to the picture on p. 105 of the book, find the ratio of the areas of the star ACEBD and the small pentagon FGHIJ.

The key point is to notice similarity of the triangles DAC and CDH (due to the equality of angles $\angle DAC = \pi/5 = \angle CDB$). Taking $|DC|$ for the unit of length and denoting $|CH| = x$ we obtain the "golden ratio" proportion $x/1 = 1/(1+x)$ and find $x = (\sqrt{5}-1)/2$. Then, taking the triangle IDJ for the (new!) unit of area, we find the area of JIH equal x, the area of JAH equal $(1+x)^2$ and the area of $JFGH$ equal $(1+x)^2-1 = 2x+x^2$. Thus in these units the area of the pentagon is $3x + x^2 = \sqrt{5}$ and the area of the star is $5 + 3x + x^2 = 5 + \sqrt{5}$. Therefore the ratio in question is equal to $\sqrt{5}+1$.

10.13+10.14. If m is not divisible by prime p then $(p, m) = 1$ and by Euclid's Lemma $1 = kp + lm$ for some k and l. Then $n = kpn + lmn$ is divisible by p whenever mn is divisible by p. Moreover, taking this for the base of induction on r, and assuming that p divides the product $a_1...a_r$ with $r > 2$, but does not divide $a_1, ..., a_{r-1}$ we conclude, by the induction hypothesis, that p does not divide $m = a_1...a_{r-1}$ and therefore divides $n = a_r$ by the previous argument.

Homework 11.

11.7d. In $\mathbf{Z}[x]$, the divisors of x are x and 1, and the divisors of 2 are 2 and 1. Thus the only common divisor of x and 2 is 1, but it cannot be written in the form $d(x) = 2r(x) + xs(x)$ with $r, s \in \mathbf{Z}[x]$. Indeed, $d(0) = 2r(0) \in 2\mathbf{Z}$ is even, and therefore $d \neq 1$ which is odd.

11.16. Applying Euclid's lemma to $f, g \in F[x]$, we find their greatest common divisor $h(x) = r(x)f(x) + s(x)g(x) \in F[x] - \{0\}$. Put $x = \alpha \in E \supset F$. Since $f(\alpha) = g(\alpha) = 0$, we find $h(\alpha) = 0$. Thus we the greatest common divisor of f and g is non-constant.

11.19. An elementary step in the "long division" of $x^m - 1$ by $x^n - 1$ for $m \geq n$ consists in replacing $x^m - 1$ with the remainder $(x^m - 1) - x^{m-n}(x^n - 1) = x^{m-n} - 1$. In other words, it is equivalent to replacing the pair m, n with $m - n, n$ which is an elementary step in the "long division" of m by n. Thus the ultimate remainder upon division of $x^m - 1$ by $x^n - 1$ is $x^r - 1$ where r is the remainder upon division of m by n. In particular, the remainder $x^r - 1$ is zero if and only if $r = 0$.

11.20ab. Here are factorizations of $x^n - 1$ (with $\Phi_n(x)$ in bold) for $1 \leq n \leq 12$:
$(\mathbf{x - 1})$, $(x - 1)(\mathbf{x + 1})$, $(x - 1)(\mathbf{x^2 + x + 1})$, $(x - 1)(x + 1)(\mathbf{x^2 + 1})$,
$(x - 1)(\mathbf{x^4 + x^3 + x^2 + x + 1})$, $(x - 1)(x + 1)(x^2 + x + 1)(\mathbf{x^2 - x + 1})$,
$(x - 1)(\mathbf{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1})$,
$(x - 1)(x + 1)(x^2 + 1)(\mathbf{x^4 + 1})$, $(x - 1)(x^2 + x + 1)(\mathbf{x^6 + x^3 + 1})$,
$(x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(\mathbf{x^4 - x^3 + x^2 - x + 1})$,
$(x - 1)(\mathbf{x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1})$,
$(x - 1)(x + 1)(x^2 + 1)(x^2 + x + 1)(x^2 - x + 1)(\mathbf{x^4 - x^2 + 1})$.
This table suggests that $x^n - 1 = \prod_{d|n} \Phi_d(x)$, and that $\deg \Phi_n = \phi(n)$ (so that in particular $n = \sum_{d|n} \phi(d)$).

Homework 12.

12.6. $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ means $a = b + kn, c = d + ln$ for some $k, l \in \mathbf{Z}$. Then $a + c = b + d + (k + l)n$ and $ac = bd + (bl + ck + kl)n$ and hence $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

12.10. $\phi(1) = 1$ (by definition), $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$, $\phi(11) = 10$, $\phi(12) = 4$, $\phi(13) = 12$, $\phi(14) = 6$, $\phi(15) = 8$, $\phi(16) = 8$, $\phi(17) = 16$, $\phi(18) = 6$, $\phi(19) = 18$, $\phi(20) = 8$, $\phi(21) = 12$, $\phi(22) = 10$, $\phi(23) = 22$, $\phi(24) = 12$.

12.11. When p is prime $\phi(p^n) = p^n - p^{n-1}$ since among the p^n remainders $0, 1, 2, ..., p^n - 1$ those and only those p^{n-1} which are multiples of p are not relatively prime to p.

12.17b. The Euclidean algorithm for $1 = (147, 17)$ yields the remainders: $11 = 147 - 8 \cdot 17$, $6 = 17 - 11$, $5 = 11 - 6$, $1 = 6 - 5$. Thus

$$1 = 2 \times 6 - 11 = 2 \cdot 17 - 3 \cdot 11 = 26 \cdot 17 - 3 \cdot 147.$$

Thus $26 \cdot 17 \equiv 1 \pmod{147}$.

12.24. $U_5 := (\mathbf{Z}/5\mathbf{Z})^\times$ is cyclic of order 4 generated by 2:

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 \equiv 3, 2^4 \equiv 1 \pmod{5}.$$

The group U_8 is isomorphic to the Cartesian product of two cyclic groups of order 2 since squares of all elements in U_8 equal 1:

$$1^2 = 1, 3^2 = 9 \equiv 1, 5^2 = 25 \equiv 1, 7^2 = 49 \equiv 1 \pmod{8}.$$

Homework 13.

1. Prove that the group of units of any finite field is cyclic.

Let $G = F^\times$ be the group of units of a finite field F of cardinality q. Let r be the *exponent* of the group G, i.e. the minimal positive integer such that $a^r = 1$ for all $a \in G$. Since G is abelian, it contains a cyclic subgroups of cardinality r (as we proved in the class by constructing an element of order $L.C.M.(m,n)$ out of two elements of orders m and n). Thus it suffices to show that $a^r = 1$ cannot hold true for all $a \in G$ if $r < q-1$. But this follows from the fact that the polynomial $x^r - 1 \in F[x]$ cannot have $q - 1 = |G|$ distinct roots when its degree $r < q - 1$.

13.13. Any non-identity element in a group G generates a non-trivial cyclic subgroup whose cardinality divides that of G (by Lagrange's theorem). When the latter cardinality is prime, this cyclic subgroup coincides therefore with the whole group.

12.30. The *cyclotomic polynomial* $\Phi_n(x)$ is defined as the monic polynomial whose roots are primitive complex n-th roots of 1. All n-th roots of 1 form in $\mathbf{C}^\times$ a cyclic subgroup C_n of order n. Each n-th root ξ of 1 is a primitive root of order d equal to the cardinality of the cyclic subgroup generated by ξ. In particular, d is a divisor of n (by Lagrange's theorem). Vice versa, when $d|n$, primitive d-th roots of 1 are n-th roots of 1 as well. Thus

$$\prod_{d|n} \Phi_d(x) = \prod_{\xi \in \mathbf{C}:\ \xi^n = 1} (x - \xi) = x^n - 1,$$

and $\deg \Phi_n = \phi(n)$, the number of generators in C_n. Since $\Phi_1 = x - 1$ has integer coefficients, it follows by induction on n that Φ_n has integer coefficients too. Indeed, by the induction hypothesis we may assume that $P_n := \prod_{d|n, d<n} \Phi_d$ is a monic polynomial with integer coefficients. The $\Phi_n = (x^n - 1)/P_n$ has integer coeffcients too since the long division algorithm by a *monic* polynomial produces no fractional coefficients.

Homework 14.

14.18. Let $n = a^2 + b^2$ be diviible by a prime p of the form $4k - 1$. Then p remains prime in $\mathbf{Z}[i]$, n factors as $(a + ib)(a - ib)$ in $\mathbf{Z}[i]$ and therefore p divides at least one of $a \pm ib$ by the definition of prime elements. Thus both a and b are divisible by p and n is divisible by p^2 and hence is *not* square-free. In other words, a square-free product $n = p_1...p_r$ of prime numbers containing a prime of the form $4k - 1$ is not the sum of two squres. Vice versa, if none of the prime factors is of the form $4k - 1$, then each of them can be written as the sum of two squares (by Fermat's result) and thus $n = a^2 + b^2$ for some natural a and b too. Indeed, when $x = (\alpha + i\beta)(\alpha - i\beta)$ and $y = (\gamma + i\delta)(\gamma - i\delta)$ then $xy = (a + ib)(a - ib)$ with $a + ib = (\alpha + i\beta)(\gamma + i\delta)$.

16.5. To divide the circle into $n = 2, 3, 4, 6, 8, 12$ equal parts using straightedge and compass, for $n = 2$ — produce a diameter, for $n = 4$ — produce the diameter perpendicular to the first one; for $n = 6$ — use the arcs subtended by the chords equal to the radius of the circle, for $n = 3$ — use every 2nd vertex of the 6-gon, for $n = 8, 12$ — bisect the arcs constructed respectively for $n = 4, 6$.

16.15. If α is a real root of a cubic polynomial irredicuble in $\mathbf{Q}[x]$ then the extension field $F = \mathbf{Q}(\alpha)$ has dimension 3 as a vector space over $\mathbf{Q}$. If $E \supset F$ is a field of dimension m over $\mathbf{Q}$ then $m = 3 \dim_F E$ is divisible by 3. On the other hand, if α is constructible, then it belongs to an extension field $E \supset \mathbf{Q}$ obtained from $\mathbf{Q}$ by consecutive adjoinig roots of quadratic polynomials with previously constructed coefficients. Thus $\dim_{\mathbf{Q}} E$ is a power of 2 and is not divisible by 3.

16.17. We have $1 = 2 \times 3 - 1 \times 5$ and hence $1/15 = 2/5 - 1/3$. The angle $2\pi/15$ can therefore be constructed by duplicating the central angle $2\pi/5$ of the regular pentagon and subtracting the central angle $2\pi/3$ of the regular triangle.

18.14. Let $t = \xi + \xi^{-1}$ where $\xi = \cos(2\pi/7) + i \sin(2\pi/7)$ is the primitive 7-th root of 1. Then $t^2 = \xi^2 + 2 + \xi^{-2}$, $t^3 = \xi^3 + 3\xi + 3\xi^{-1} + \xi^{-3}$ and therefore

$$t^3 + t^2 - 3t - 1 = \xi^3 + \xi^2 + \xi + 1 + \xi^{-1} + \xi^{-2} + \xi^{-3} = 0.$$

The polynomial $x^3 + x^2 - 3x - 1$ has no rational roots (since none of $x = \pm 1$ is a root) and is therefore irreducible in $\mathbf{Q}[x]$. Thus t is a root of an irreducible over $\mathbf{Q}$ cubic polynomial and is not constructible by 16.5.