Answers to HW1

2. For a transitive and reflexive but not symmetric binary relation, one can take $\leq$; for transitive and symmetric but not reflexive, take the empty relation on any non-empty set; for reflexive and symmetric but not transitive, take the relation on the set of words of the English language, to have a letter in common.

3. $G.C.D.(1763, 991) = 1 = 181 \times 1763 - 322 \times 991$, and hence $991^{-1} \equiv -322 \equiv 1441 \mod 1763$.

4. On $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, the norm $N(a + b\sqrt{-5}) := (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$ takes values $0, 1, 4, 5, 6, \ldots$, but cannot be equal 2 or 3. Therefore 2 and 3, which divide $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$ but don't divide $1 \pm \sqrt{-5}$, are not prime. However, they are irreducible, since $N(2) = 4$ and $N(3) = 9$ cannot be factored into the product of norms $N(\alpha)N(\beta)$ in any nontrivial way, i.e. with both $N(\alpha), N(\beta) > 1$.

11. A permutation of A, B, C, D inducing a trivial permutation of V, H, S must keep vertical edges vertical, horizontal horizontal, and diagonals diagonal, i.e. must come from a geometric symmetry of the rectangle: reflection about horizontal axis (Rh), vertical axis (Rv), their composition (which is the central symmetry, Cs or equivalently the rotation through 180°), or the identity Id. Composing these four with any particular permutation σ of A, B, C, D will permute H, V, S the same way. Thus, all $4! = 24$ permutations of A, B, C, D are partitioned into groups of four, where σ and σ' are in the same group whenever $\sigma^{-1}\sigma' \in \{Rh, Rv, Cs, Id\}$. The last condition is equivalent to saying that σ and σ' induce the same permutation of V, H, S. Since $24/4 = 3!$, each permutation of V, H, S is so induced four times.

HW2.

14. A and D are cyclic (3 and i can be taken for generators of order 4), while all the others are not (i.e. all non-identity elements there have order 2), and therefore are all isomorphic to the Klein group K_4.

15. All the four groups are isomorphic to S_3.

The rotation group of the triangular prism coincides with the symmetry group of a regular triangle and is identified with S_3 by numbering the triangle's vertices by 1,2,3.

$GL_2(\mathbb{Z}_2)$ consists of 6 matrices

$$\left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right], \left[\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right], \left[\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array}\right], \left[\begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array}\right], \left[\begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array}\right], \left[\begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array}\right].$$

They act naturally by automorphisms of the group C from problem 1 (the 2-dimensional vector space over $\mathbb{Z}_2$), and thus permute the 3 non-zero vectors. Since the only matrix which leaves each 2-vector fixed is the identity one, our homomorphism $GL_2(\mathbb{Z}_2) \to S_3$ is bijective.

In S_3, the transpositions $\alpha = (1\ 2)$ and $\beta = (2\ 3)$ satisfy $\alpha^2 = \beta^2 = id = (\alpha\beta)^3$ (since $(1\ 2)(2\ 3)$ is the cyclic permutation of $1, 2, 3$). This defines an onto homomorphism $K \to S_3 : a \mapsto \alpha, b \mapsto \beta$. So, it suffices to check that the group K has at most 6 elements. To this end, note that any word in K containing fragments aa or bb can be made shorter, and since $aba = bab$, any word of > 3 letters also can be made shorter by reducing the fragments: $abab = babb = ba$ or $baba = bbab = ab$. Therefore all words reduce in the group to one of the six: $\emptyset, a, b, ab, ba, aba = bab$.

HW3

19. As it follows from the division with remainder algorithm, every subgroup in $\mathbb{Z}$ consists of all multiples, $n\mathbb{Z}$, of some $n \geq 0$. Consequently, a subgroup in $\mathbb{Z}/N\mathbb{Z}$ is generated by one element, the image of the generator n of the inverse image of this subgroup in $\mathbb{Z}$.

21. In the subgroup group $\mathbb{Z}_n \subset D_n$ of rotations, every subgroup $\mathbb{Z}_k$ (and there is unique such subgroup for every $k|n$) is normal, since conjugations by reflections (which merely reverse the orientation of the plane) transform every rotation into the inverse rotation. The quotient $D_n/\mathbb{Z}_k$ for $n/k = 1$ is isomorphic to $\mathbb{Z}_2$, for $n/k = 2$ to the Klein group, and for $n/k > 2$ to the dihedral group $D_{n/k}$.

A normal subgroup H in D_n containing a reflection, for odd n, contains all reflections (which form a single conjugacy class in D_n) and hence coincides with D_n (so that D_n/H is the trivial group. For even n, reflections in D_n form 2 conjugacy classes, and H can contain one of them or both. In the latter case, $H = D_n$ as for n odd, but in the former case H must contain the half of all rotations, and hence $D_n/H \cong \mathbb{Z}_2$.

40. We've found out with you in class that the rotation group G of the cube contains: 8 rotations through 120° (in either direction about each of the 4 diagonals), which fit into 4 cyclic subgroups of order 3; 6 rotations through 90° (in either direction about each of the three axes) fitting 3 cyclic subgroups of order 4; 3 cyclic subgroup of order 2 generated by rotations through 180° about these exes, and 6 more cyclic subgroups of order 2 generated by 180° rotations about the lines passing through midpoints of opposite edges (so, totally 9 subgroups isomorphic to $\mathbb{Z}_2$). Together with the cyclic subgroup of the identity, this covers all the $8 + 6 + 3 + 6 + 1 = 24$ elements of G. None of these subgroups is normal because conjugations, don't preserve, but permute the subgroups of each kind (e.g. rotations about one diagonal become rotations about another diagonal, and so on).

47. Since composite divisors of 24 are $24, 12, 8, 6, 4$, these are the possible orders of non-cyclic subgroups $H \subset G$. When $|H| = 12$, H has only 2 cosets, H and H^c, both therefore left and right, so that H is normal: it is the alternating group $A_4 \subset S_4 \cong G$. Now, think of the cube as a thick square: the dihedral group D_4 of symmetries of this square can be realized by rotations of the square in space. This yields 3 subgroups of order 8, depending on which of the 3 dimensions of the cube is viewed as its "thickness". The symmetry group D_4 of a square has 2 non-cyclic subgroups of order 4: one generated by reflections about the diagonals of the square, the other about the "axes" of the

square. In fact the three subgroups of the former kind thus obtained are different, while the three subgroups of the latter kind coincide with the normal Klein subgroup in G (it contains the 180° rotations about the cube's exes). Four subgroups of order 6 are easy to describe via the identification $G \cong S_4$, since obviously S_4 has 4 subgroups isomorphic to S_3, each fixing one of the 4 objects (i.e. one of the 4 diagonals of the cube, in the geometric realization).

For $|H| = 4$, the normal Klein subgroup is isomorphic of course to the other 3 non-cyclic subgroups of order 4, but not conjugated to them. In the other cases, the non-cyclic subgroups of the same order are conjugated to each other (as should be clear from their uniform, and therefore conjugation-invariant description).

In fact we are lacking some bits of general theory to guarantee that the found examples of non-cyclic subgroups of given orders are all such subgroups. So, the difficulties in completing this problem should serve as a motivation for further development of that general theory.

HW4.

38. (a) K is invariant under conjugations by elements of H because it is invariant under conjugaions by all elements of $G \supset H$. (b) The homomorphism $\pi : G \to G/K$ restricted to (any subgroup) $H \subset G$ is still a group homomorphism, and so its range is a subgroup. (c) The homomorphism $\pi|_H : H \to G/K$, as any group homomorphism, factors as the composition of the the canonical projection $H \to H/\ker(\pi|_H)$, an isomorphism between $\ker(\pi|_H) \cong \pi(H)$ and the inclusion $\pi(H) \subset G$. But $\ker(\pi|_H) = H \cap \ker(\pi) = K$ since $H \supset K$.

50. If the sequence $\sigma(1), \ldots, \sigma(n)$ is increasing, then $\sigma = \mathrm{id}$. Otherwise there is a pair of nearby indices $i, i+1$ such that $\sigma(i) > \sigma(i+1)$. Then the length $l(\sigma\tau_{i,i+1}) = l(\sigma) - 1$, where $\tau_{i,i+1} = (i\ i+1)$. (Indeed, all other than $i, i+1$ pairs of indices are in inversion for σ whenever they are in inversion for $\tau_{i,i+1}\sigma$.) Thus, after precomposing σ with some sequence of $l(\sigma)$ transpostions of suitable nearby indices, we obtain a permulation of length $l = 0$, i.e. id. Therefore, σ is the product of the inverse sequence of $l(\sigma)$ transpositions of nearby indices.

56. In case (i) the order $|H| = 1 + (p-1)!/2$ divides $p!/2$, i.e. $(1 + (p-1)!/2)m = p\ , (p-1)!/2$ for some m. Note that $(p-1)!/2$ is coprime with $1 + (p-1)!/2$, and hence $m = l(p-1)!/2$ for some l. Since p is prime, we find that $l = 1$, and therefore $p = 1 + (p-1)!/2$. Starting from $p = 5$ the R.H.S. is greater than p, and for $p = 3$, the R.H.S. equals $2 \neq p$.

Similarly, in case (ii) the order $|H| = 1 + (p+1)\,(p-1)!/2$ divides $(p+1)!/2$, i.e. $(1+(p+1)\,(p-1)!/2)m = p\,(p+1)\,(p-1)!/2$ for some m, Since $(p+1)\,(p-1)!/2$ is coprime with $1+(p+1)\,(p-1)!/2$, we find that $m = l\,(p+1)\,(p-1)!/2$ where actually $l = 1$, i.e. $p = 1+(p+1)\,(p-1)!/2$. Here the R.H.S. is greather than p staring from $p = 3$.

Thus, both situations (i) and (ii) lead to contradictions.

57. Commutator subgroup $[G, G]$ of a group G is normal since it is defined (as the smallest subgroup containing all commultators $xyx^{-1}y^{-1}$ of the group's elements) in a way invariant under all automorphisms of the group (including therefore interior automorphisms). It is also smallest normal subgroupquotient by which is abelian (since a homomorphism from G to an abelian group contains all commutators in its kernel). For $n > 4$, A_n is simple (i.e. has no proper normal subgroups except $\{e\}$, and is non-abelian (hence $[A_n, A_n] \neq \{e\}$), leaving the only option $[A_n, A_n] = A_n$. Since commutators of any permutations are even, $[S_n, S_n] \subset A_n$, and actually $= A_n$ for all $n > 1$, since even for $n = 4$, $S_4/K_4 \cong S_3$ is non-abelian (and the cases $n = 3$ and $n = 2$ are obvious).

HW5.

64. In a group G of order p^2, a non-central element commutes with (at least p yet fewer than p^2 and hence) p elements, and therefore its conjugacy class must contain $p^2/p = p$ elements. Therefore the order of the center $Z(G)$ must be also divisible p, and if it is p^2, then the groups is abelian. But assuming that it is not leads to a contradiction, since any non-central element must commute with $Z(G)$ and with itself, i.e. with more than p elements.

66. The identity rotation fixes all the $3^6 = 729$ 3-colorings of the cube. Each of the 8 rotations through 120° fixes 3^2 colorings. Each of the 6 rotations through 180° around the midlines of opposite edges fixes 3^3 colorings. Each of the 3 rotations through 180° around the "coordinate" axes of the cube fixes 3^4 colorings. Each of the 6 rotations through 90° about those 3 axes fixes 3^3 colorings. So, the total number of orbits equals

$$\frac{1}{24}(3^6 + 8 \cdot 3^2 + 6 \cdot 3^3 + 3 \cdot 3^4 + 6 \cdot 3^3) = 57.$$

A: *Prove that any finite group is isomorfic to a subgroup of A_n for some n.* By Cayley's theorem, any group G (finite or not) can be realized by permutations σ_g on itself (e.g. by means of the action by left translations). When $|G| < \infty$, realize G by permutations (σ_g, σ_g) on $G \times G$: even when σ_g is odd, $(\sigma_g, \sigma_g) = (\sigma_g, \mathrm{id})(\mathrm{id}, \sigma_g)$ will be even.

B: *Prove that a group of order 45 is abelian.* A group G of order 45 contains two Sylow's subgroups: G_1 of order 9, abelian by problem 64, and G_2 of order 5, isomorphic to $\mathbb{Z}_5$. The number of Sylow's p-subgroups (as they all are conjugated by the 2nd Sylow theorem) is a divisor of $|G|$, which (by the 3rd Sylow theorem) is $\cong 1 \mod p$. The only divisor of 45 which is $1 \mod 5$ or $1 \mod 3$ is 1, implying that G_1 and G_2 are unique, and hence normal. Obviously $G_1 \cap G_2 = \{e\}$, which implies that the subgroups commute. Indeed, for $x \in G_1$ and $y \in G_2$, we have $G_2 \ni (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in G_1$, i.e. the commutator equals e. Thus $G = G_1 \times G_2$, the direct product of abelian groups, and thus G is abelian.

HW6

78. Call a vector in the lattice $\mathbb{Z}^2$ *divisible* if it is an integer multiple of some shorter vector. Let $H \subset \mathbb{Z}^2 = \{(x,y)|x,y \in \mathbb{Z}\}$ be a non-zero subgroup, $v \in H$ a vector indivisible in H, and if it is divisible in $\mathbb{Z}^2$, then let v_0 will be a vector indivisible in $\mathbb{Z}^2$ proportional to v. The quotient of $\mathbb{Z}^2$ by $\mathbb{Z}v_0$ is free (because the opposite would mean that v_0 is divisible), and hence isomorphic to $\mathbb{Z}$. The projection of H to $\mathbb{Z}^2/\mathbb{Z}v_0$ is a subgroup in $\mathbb{Z}$, and therefore, by the division-with-remainder algorithm, has the form $d\mathbb{Z}$ for some d, i.e. is isomorphic to either $\mathbb{Z}$ or $\{0\}$. The kernel of the projection of H onto $d\mathbb{Z}$ is $\mathbb{Z}v$. When $d = 0$, $H = \mathbb{Z}v \cong \mathbb{Z}$. When $d \neq 0$, the projection possesses a right inverse (because $d\mathbb{Z}$ is free), thereby representing H as the direct sum $d\mathbb{Z} \oplus \mathbb{Z}v \cong \mathbb{Z}^2$.

Remark: Likewise, using induction on n, one can prove that any subgroup in $\mathbb{Z}^n$ is finitely generated and is therefore isomorphic to one of $\mathbb{Z}^k$ with $k = 0, 1, \ldots, n$.

86. Let A be a finite abelian p-group $\cong \mathbb{Z}_{p^{a_1}} \oplus \mathbb{Z}_{p^{a_2}} \oplus \cdots$. The *columns* of the Young diagram whose *rows* have lengths $a_1 \geq a_2 \geq \cdots$ have heights $m_1 \geq m_2 \geq \cdots$ which can be described as follows: p^{m_k} is the number of elements x in the subgroup $p^{k-1}A$ which satisfy $px = 0$. (Note that the Young diagram for $p^{k-1}A$ is obtained from that for A by erasing the $k-1$ leftmost columns.) When B is a subgroup in A, $p^{k-1}B \subset p^{k-1}A$, and hence the number of solutions to $px = 0$ in B does not exceed the number of such solutions in A. Therefore the heights $n_1 \geq n_2 \geq \cdots$ of the columns of the Young diagram whose rows have lengths $b_1 \geq b_2 \geq \ldots$ satisfy $n_l \leq m_l$ for all l. This implies that the whole Young diagram for B *fits inside* the Young diagram for A. In particular, the lengths of the rows of these two diagrams also satisfy $b_k \leq a_k$ for all k.

87. In $\mathbb{Z}_{17}^\times$, if $x \equiv \pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8$,
then $x^2 \equiv 1, 4, -8, -1, 8, 2, -2, -4$ respectively. Thus, $x^2 = 1$ has only two solutions $x \equiv \pm1$, guaranteeing that the group is cyclic.

In $\mathbb{Z}_{32}^\times$, if $x \equiv \pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13, \pm15$,
then $x^2 \equiv 1, 9, -7, -15, -15, -7, 9, 1$ respectively. Therefore $x^2 = 1$ has 4 solutions $(\pm1, \pm15)$, $x^4 = 1$ has 2^3 solutions (the 4 more are ±7 and ±9), and consequently $x^8 = 1$ is satisfied by all 2^4 elements of the group. Thus, the columns of the Young diagram have heights $2+1+1$, and hence the rows have lengths $3+1$: $\mathbb{Z}_{32}^\times \cong \mathbb{Z}_8 \oplus \mathbb{Z}_2$.

91. The center $Z \subset G$ of the group (which consists of the one-element conjugacy classes) must have $mod 2$ as many elements as the group, i.e. $8, 4, 2$ but not 1. The first possibility means that the group is abelian, and hence is isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathcal{Z}_2$, $\mathbb{Z}_2^3$ (according to partitions of $3 = 3 = 2 + 1 = 1 + 1 + 1$, per our classification of finite abelian p-groups.) The second possibility ($|Z| = 4$), leads to a contradiction, because $g \in G - Z$ must commute with itself and all elements of the center, and hence must commute with all elements of G, i.e. $g \in Z$. For the same reason, when $Z \cong \mathbb{Z}_2$, the quotient G/Z cannot have elements g of order 4, and thus must be isomorphic to the Klein $\mathbb{Z}_2^2$. Now the question is how many different (non-abelian) groups G one can assemble from $\mathbb{Z}_2$ as the center and $\mathbb{Z}_2^2$ as the quotient by it.

The answer is two, up to isomorphism: D_4, the symmetry groups of the square, and the group Q of unit quaternions: $\{\pm 1, \pm i, \pm j, \pm k\}$. They are not isomorphic: Q has only one element of order 2 (the central one), and D_4 has 4 more (the reflections).

To prove this, represent the center as $\{\pm 1\}$, and let a and b denote two non-central element from different Z-cosets. Then all elements of the group have the form $\pm 1, \pm a, \pm b, \pm ab$, and moreover, $ba = -ab$, since when $ba = ab$, the whole group turns out to be abelian. In the case that none of $\pm a, \pm b, \pm ab$ has order 2, their squares must be -1, which yields the multiplication table of the group Q: $a^2 = b^2 = (ab)^2 = ab(ab) = -1$. Now let $a^2 = 1$. Then $b^2 = baab = -(ab)^2$, i.e. either $b^2 = 1$, $(ab)^2 = -1$, or the other way around. In the first case we get the multiplication table of D_4, with reflections $\pm a, \pm b$, and rotations $\pm ab, \pm 1$. The other case $b^2 = -1$, $(ab)^2 = 1$ leads to an isomorphic group: put $c = ab$, and conclude that $ac = a^2 b = b$, i.e. $a^2 = c^2 = 1$ and $(ac)^2 = -1$.

HW7

99. In $\mathbb{R}[S_2] = \{a\,\mathrm{id} + b\tau \mid a, b \in \mathbb{R}\}$, where τ is the transposition, take the basis $e_\pm = (\mathrm{id} \pm \tau)/2$. We have: $e_+e_- = e_-e_+ = (\mathrm{id}^2 - \tau^2)/4 = 0$, and

$$e_\pm^2 = \frac{\mathrm{id}^2 \pm 2\,\mathrm{id}\,\tau + \tau^2}{4} = \frac{\mathrm{id} \pm \tau}{2} = e_\pm.$$

Therefore the multiplication in this basis is the same as in the standard basis of $\mathbb{R}^2$: $(1,0)(0,1) = (0,0)$, $(1,0)^2 = (1,0)$, $(0,1)^2 = (0,1)$.

119. Let $Z = F \cup G$ be the union of two algebraic sets given respectively by equations $\{f_\alpha = 0\}$ and $\{g_\beta = 0\}$. Then the equations $f_\alpha g_\beta = 0$ define Z. Indeed, if $(x_0, y_0) \notin Z$, then$f_{\alpha_0}(x_0, y_0) \neq 0$ for some α_0 and $g_{\beta_0}(x_0, y_0) \neq 0$ for some β_0, and hence $f_{\alpha_0} g_{\beta_0} \neq 0$ at (x_0, y_0). Conversely, if $(x_0, y_0) \in Z$, then either $(x_0, y_0) \in F$, in which case $f_\alpha(x_0, y_0) = 0$ for all α, or $(x_0, y_0) \in G$, in which case $g_\beta(x_0, y_0) = 0$ for all β. In either case all $f_\alpha g_\beta$ vanish at (x_0, y_0). Since any one-point set $\{(x_0, y_0)\}$is algebraic (given by the equations $x - x_0 = 0, y - y_0 = 0$), any finite set is also algebraic.

120. If a degree-2 polynomial $F(x, y)$ factors into the product $A(x, y)B(x, y)$ of degree-1 polynomials, the zero locus $F(x, y) = 0$ is the union of two lines, $A = 0$ and $B = 0$, not necessarily distinct. Since $x^2 + y^2 = 1$ is not a union of lines, the polynomial is irreducible, hence prime (assuming the uniqueness of factorization) implying that $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ is an integral domain.

In $\mathbb{R}^2$, the locus $x^2 + y^2 = 0$ is a point, not the union of lines, and hence $\mathbb{R}[x, y]/(x^2 + y^2)$ is an integral domain too. However, over $\mathbb{C}$ we have $x^2 + y^2 = (x + iy)(x - iy)$, and so $\mathbb{C}[x, y]/(x^2 + y^2)$ is not an integral domain.

Likewise, over $\mathbb{Z}_5$ we have $x^2+y^2 = (x+2y)(x-2y)$, i.e. $\mathbb{Z}_5/(x^2+y^2)$ is not an integral domain. However, in $\mathbb{Z}_{11}$ there is no square root of -1, implying that $x^2 + y^2$ is irreducible, hence prime (again, relying on uniqueness of factorization in $\mathbb{Z}_5[x, y]$, and so $\mathbb{Z}_{11}/(x^2 + y^2)$ is an integral domain.

121. *Answer:* (c) $\cong$ (e), (b) $\cong$ (d).

In $\mathbb{Z}[x]$, $2x^2 - 6 = (2x + 4)(x - 2) + 2$, i.e. $I := (x^2 - 3, 2x + 4) = (x^2 - 3, 2) = ((x + 1)^2, 2)$. Therefore $\mathbb{Z}[x]/I \cong \mathbb{Z}_2[x]/((x + 1)^2) \cong \mathbb{Z}_2[y]/(y^2)$. This ring has 4 elements: $0, 1, 1 + x, x \mod (x^2)$, of which only x is not invertible. In $\mathbb{Z}_2 \times \mathbb{Z}_2$, also consisting of 4 elements, $(0, 0), (1, 1), (1, 0), (0, 1)$, the last two are not invertible, and hence (a) is not isomorphic to (b) and (d).

In $\mathbb{Z}[i]$, the ideal $(i-2)$ contains $(i-2)(i+2) = -5$, i.e. $(5) \subset (i-2) \subset \mathbb{Z}[i]$. The quotient $\mathbb{Z}[i]/(5) \cong \mathbb{Z}_5[i]$ is *additively* isomorphic to $\mathbb{Z}_5 \oplus \mathbb{Z}_5 = \{a+bi | a, b \in \mathbb{Z}_5\}$. In this quotient, $i-2$ is neither zero, nor invertible (since it is a zero divisor). Thus, the quotient $\mathbb{Z}[i]/(i-2)$ is *additively* isomorphic to $\mathbb{Z}_5$. The *ring* homomorphism $\mathbb{Z} \mapsto \mathbb{Z}[i]/(i-2)$, defined by mapping 1 to $1 + (i-2)$ has kernel $5\mathbb{Z}$. Indeed, if an ordinary integer n is divisible in $\mathbb{Z}[i]$ by $i-2$, i.e. $n = (i-2)(a+bi)$, then $n^2 = 5(a^2+b^2)$, hence $5|n^2$ in $\mathbb{Z}$, hence $5|n$. Thus the *ring* homomorphism $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}[i]/(i-2)$ is well-defined, injective and therefore bijective.

On the other hand, identify $\mathbb{Z}_5[x]/(2x+4)$ with $\mathbb{Z}_5[y]/(y)$ by the change of variable $y = 2x+4$, invertible since 2 is invertible in $\mathbb{Z}_5$: $x = (y-4)/2 = 3y-2$.

Clearly, $\mathbb{Z}_5[y]/(y) \cong \mathbb{Z}_5$ (and not isomorphic to (d) since it has 5 elements, not 4).

HW8.

126. If $m = kn + r$ where $0 < r < n$, then $a^m = (a^n)^k a^r = b^m = (b^n)^k b^r$ and since $a^n = b^n$, by cancellation rule in an integral domain, we have $a^r = b^r$. Then, by the Euclidean algortithm for integers, $a^{G.C.D(m,n)} = b^{G.C.D.(m,n)}$, i.e. $a = b$ when $G.C.D.(m, n) = 1$.

127. When $m \geq n$, we have $x^m - 1 = x^{m-n}(x^n - 1) + x^{m-n} - 1$. Consequently, if $m = kn + r$ where $0 \leq r < n$, we find that the remeinder of the division of $x^m - 1$ by $x^n - 1$ is equal to $x^r - 1$. Therefore, by the Euclidean algorithm for polynomials, $G.C.D(x^m - 1, x^n - 1) = x^{G.C.D.(m,n)} - 1$.

128. The ring $\mathbb{Z}[\zeta]$ can be visualized as a parallelogram lattice $\mathbb{Z} + \mathbb{Z}\zeta$, i.e. as the tiling of $\mathbb{C}$ by integer translated of the parallelogram (actually rhombus) with the vertices $0, 1, 1 + \zeta, \zeta$. In fact this rhombus consists of two equilateral triangles: one with vertices $0, 1, 1 + \zeta$ and $0, 1 + \zeta, \zeta$. A principal ideal $(a_0 + b_0\zeta)$ generated by $a_0 + b_0\zeta$ is obtained therefore by myltiplying this lattice by $a_0 + b_0\zeta$, and can be visualized as a similar tiling of $\mathbb{C}$ by equilateral triangles obtained from the previous one by rotating through $\arg(a_0 + b_0\zeta)$ and stretching by $l := |a_0 + b_0\zeta|$. Note that each point in an equilateral triangle with the side length l lies within the distance $l/\sqrt{3}$ of one of the triangle's vertices. Consequantly every complex number z lies within the distance $l/\sqrt{3} < l$ of one of the points in the ideal $(a_0 + b_0\zeta)$. This implies that $\mathbb{Z}[\zeta]$ is a Euclidean ring with the "distance" finction d given by the squared absolute value of complex numbers: $d(a + b\zeta) = (a + b\zeta)(a + b\overline{z}) = a^2 - ab + b^2$.

129. The ring $\mathbb{Z}[\sqrt{-3}]$ can be visialized as the rectangular lattice is the complex plane $\mathbb{C}$ with a basis 1 and $\sqrt{3}i$. The diagonal in a rectangle with the side lenghth l and $\sqrt{3}l$ has length $2l$. Therefore the center of the reclangle lies at the distance from all of its vertices exactly *equal* to l (and not *smaller* than l, which would be needed to show that the "distance" function $d(z) = |z|^2$ turns the ring into a Euclidean one).

HW9.

130. If $f \in \mathbb{Z}_2[x]$ is an irreducible polynomial of defree n then $\mathbb{Z}_2[x]/(f)$ is a field (since in a PID the ideal (f) maximal among principal ideals is maximal) and has 2^n elements (since $1, x, \dots, x^{n-1}$ form its basis as a vector space over $\mathbb{Z}_2$). In degrees 2 and 3, irreducible polynomials are those which have no roots in $\mathbb{Z}_2$, i.e. x^2+x+1, x^3+x^2+1 and x^3+x+1. In degree 4, a reducible polynomial ether has a root in $\mathbb{Z}_2$, or is $(x^2+x+1)^2 = x^4+x^2+1$. Therefore $\mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{Z}_2[x]/(x^3+x+1)$ and $\mathbb{Z}_2[x]/(x^4+x+1)$ are fieds consistingg of 4, 8, and 16 elements respectively.

136.(b) For $S = \{x^k \mid k > 0\}$, $\mathbb{C}[x]_S$ consists of rational functions whose denominators do not vanish anywhere except x. They have the form $a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 + a_{-1}x^{-1} + \dots + a_{-m}x^{-m}$ and are called *Laurent polynomials*. In the latter case this is the ring "polynomial" (the official term is "regular") functions on $\mathbb{C} - \{0\}$.

(a) For $S = \mathbb{C}[x] - (x)$, $\mathbb{C}[x]_S$ consists of rational functions with denominators not divisible by x (i.e. non-vanishing at $x = 0$). The only point where the values of all those rational functions are well-defined is $x = 0$, and the whole ring can be interpreted as the ring of "regular" functions in an infinitesimal neighborhood of $x = 0$.

139. Since $\mathbb{Z}$ (being a Euclidean ring) is a UFD, $\mathbb{Z}[x]$ is a UFD by the main theorem. The ideal in $\mathbb{Z}[x]$ generated by 2 and x (which consists of all polynomials f with even free term $f(0)$, and is a maximal ideal since $\mathbb{Z}[x]/(2, x) = \mathbb{Z}_2$ is a field) is not principal, since the only common factors of 2 and x are the units ± 1.

144. The polynomial $f = x^8 + x^2 + 2$ has no real roots. Therefore all its complex roots come as pairs of complex conjugate ones. Moreover, all of its complex roots are simple, since f is coprime to its derivative $f' = 8x^7 + 2x$ (as can be cheched by the Euclidean algorithm):

$$x^8 + x^2 + 2 = (x^6 + 1/4)x^2 + 3x^2/4 + 2$$
$$x^6 + 1/4 = (x^2 + 8/3)(x^4 - 8x^2/3 + 64/9) - 512/27 + 1/4$$

Therefore f factors in $\mathbb{R}[x]$ into 4 distinct irredicible quadratic polynomials. Consequently (f) is contained in 4 maximal ideals of $\mathbb{R}[x]$.

HW10

146. None of $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$ is a root of $f := 8x^3 - 6x - 1$. Therefore f is irreducible over $\mathbb{Q}$, and $\mathbb{Q}[x]/(f)$ is a field. Dividing f by $x-1$, we find that $f = (8x^2+8x+2)(x-1)+1$. Thus, $-8x^2-8x-2$ is inverse to $x-1$ modulo (f).

149. $1105 = 5 \cdot 13 \cdot 17$ can be factored in $\mathbb{Z}[i]$ as $(A+Bi)(A-Bi)$ in 4 essentially different ways with $A+Bi$ being one of the following products:

$$(2+i)(3+2i)(4+i) = (4+7i)(4+i) = 9+32i$$
$$(2+i)(3+2i)(4-i) = (4+7i)(4-i) = 23+24i$$
$$(2+i)(3-2i)(4+i) = (3-2i)(7+6i) = 33+4i$$
$$(2-i)(3+2i)(4+i) = (2-i)(10+11i) = 31+12i$$

Thus, $1105 = 33^2+4^2 = 32^2+9^2 = 31^2+12^2 = 24^2+23^2$.

154. In a direct product of finite cyclic groups, each element g belongs to the exponent d (i.e. satisfies $g^d = e$) where d is the least common multiple of the orders of these cyclic groups. This d is equal to the order of the group only when the orders of the factors are pairwise coprime, in which case the whole direct product is cyclic. If the multiplicative group $F^\times$ of a field F of q elements were not cyclic, then all $q-1$ elements $x \in F^\times$ of the group would belong to an exponent d which is smaller than $q-1$ i.e. all x would be roots of the polynomial $x^d - 1$ of degree $d < q-1$. This would contradict the fact that the degree of a polynomial cannot be smaller than the number of its roots in a given field.

160. The Taylor series of $\log 1/(1-u)$ is $u + u^2/2 + \cdots + u^k/k + \cdots$. Therefore $e^{-(u+u^2/2+\cdots+u^k/k+\cdots)} = 1-u$. Taking $u = x_i t$ and multiplying over $i = 1, \ldots, n$, we obtain Newton's identity

$$(1-x_1 t) \times (1-x_n t) = e^{-\sum_{k>0} N^k t^k/k}, \quad \text{where } N_k + x_1^k + \cdots + x_n^k.$$

Interprting the exponential function as the series $e^z = 1 + z + \cdots + z^k/k! + \cdots$, we find that the coefficient at t^k with $k > 0$ on the right is $-N_k/k +$ (lower order terms), where the "lower order terms" are polynomial expression of $N_1, \ldots, N_{k-1}$ with rational coefficeints. On the left, the coefficient at t^k is $(-1)^k \sigma_k(x_1, \ldots, x_n)$ when $k = 1, \ldots, n$ and 0 when $k > n$. For $k \leq n$, this leads to the expressions $\sigma_k = (-1)^k N_k/k +$ (lower order terms), and for $k > n$ allows one to consecutively express N_k as a rational coefficient polynomial of $N_1, \ldots, N_{k-1}$.

For $k = 1, 2, 3$ we have:

$$e^{-N_1 t - N_2 t^2/2 - N_3 t^3/3 + \cdots} =$$

$$1 - N_1 t - \frac{N_2 t^2}{2} - \frac{N_3 t^3}{3} + \frac{1}{2}\left(N_1 t + \frac{N_2 t^2}{2}\right)^2 - \frac{(N_1 t)^3}{6} + \cdots$$

$$1 - t N_1 + t^2\left(-\frac{N_2}{2} + \frac{N_1^2}{2}\right) + t^3\left(-\frac{N_3}{3} + \frac{N_1 N_2}{2} - \frac{N_1^3}{6}\right) + \cdots,$$

i.e. $\sigma_1 = N_1$, $\sigma_2 = (N_1^2 - N_2)/2$, $\sigma_3 = N_3/3 - N_1 N_2/2 + N_1^3/6$. Note that these expressions don't depend on n as long as $n \geq 3$.

HW11

162. For $0 \le k_1 < k_2$, we have

$$\begin{vmatrix} x_1^{k_1} & x_2^{k_1} \\ x_1^{k_2} & x_2^{k_2} \end{vmatrix} / \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = (x_1x_2)^{k_1} \frac{x_2^{k_2-k_1} - x_1^{k_2-k_1}}{x_2 - x_1}$$
$$= x_1^{k_2-1}x_2^{k_1} + x_1^{k_2-2}x_2^{k_1+1} + \cdots + x_1^{k_1+1}x_2^{k_2-2} + x_1^{k_1}x_2^{k_2-1}.$$

This is a homogeneous symmetric polynomial of degree $d = k_1 + k_2 - 1$ with the leading monomial $x_1^{k_2-1}x_2^{k_1}$ in the lexicographical ordering. Since any exponents with $k_2 - 1 \ge k_1 \ge 0$ can occur, these Schur polynomials form a linear basis in the space of symmetric polinomials in x_1, x_2 (and even in the free $\mathbb{Z}$-module of such polynomials over $\mathbb{Z}$, because the leading monomial occurs with the coefficient 1 invertible over $\mathbb{Z}$).

169. The powers α^0, α^1, α^2, α^3, and α^4 are equal respectively to

$$1,\ \sqrt{-2}+\sqrt{3},\ 1+2\sqrt{-6},\ 7\sqrt{-2}-3\sqrt{3},\ 4\sqrt{-6}-23.$$

Therefore $\alpha^4 - 2\alpha^2 + 25 = 0$. Also, together with α and α^3, the field $\mathbb{Q}(\alpha)$ contains $\sqrt{-2}$ and $\sqrt{3}$, and therefore coincides with

$$\mathbb{Q}(\sqrt{3}, \sqrt{-2}) = \{a + b\sqrt{3} + c\sqrt{-2} + d\sqrt{-6} \mid a, b, c, d \in \mathbb{Q}\}.$$

Let us prove accurately that $1, \sqrt{3}, \sqrt{-2}, \sqrt{-6}$ form a basis, i.e. are linearly independent over $\mathbb{Q}$, i.e. that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, or equivalently that $f = x^4 - 2x^2 + 25$ is irreducible in $\mathbb{Q}[x]$. For this, note that $\mathbb{Q}(\sqrt{3})$ does not yet contain $\sqrt{-2}$. One reason is that $\mathbb{Q}(\sqrt{3})$ is real but $\sqrt{-2}$ is not. Another argument (which would also work for $\sqrt{2}$ instead of $\sqrt{-2}$) is that if $\sqrt{-2}$ were a rational linear combination $a + b\sqrt{3}$ of 1 and $\sqrt{3}$, then either $\sqrt{3/2} \in \mathbb{Q}$ (if $a = 0$), or $\sqrt{-2} \in \mathbb{Q}$ (if $b = 0$), or by squaring we'd get $\sqrt{3} \in \mathbb{Q}$, all clearly wrong. Therefore $\mathbb{Q}(\alpha)$ is obtained from $\mathbb{Q}$ by two consecutive quadratic extensions, and must have degree 4 over $\mathbb{Q}$. Of course, $1, \alpha, \alpha^2, \alpha^3$ also form a basis in $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Since all the four roots $\pm\sqrt{1 \pm 2\sqrt{-6}} = \pm(\sqrt{-2} \pm \sqrt{3})$ of f lie in $\mathbb{Q}(\alpha)$, they define four different embeddings of $\mathbb{Q}[x]/(f)$ into $\overline{\mathbb{Q}} \subset \mathbb{C}$, which however have the same range $\mathbb{Q}(\sqrt{3}, \sqrt{-2})$.

170. Let $\alpha = \sqrt[4]{2}$. Then $x^4 - 2 = (x^2 - \alpha^2)(x^2 + \alpha^2) = (x - \alpha)(x + \alpha)(x^2 + \alpha^2)$. The roots $\pm i\alpha$ of the last factor are not in $\mathbb{Q}(\alpha)$, and hence it is irreducible. Yet, in $\mathbb{C}$, the polynomial has four roots $\pm\alpha, \pm i\alpha$, and respectively $\mathbb{Q}[x]/(x^4 - 2)$ has four embeddings. Since the field containing α would contain $-\alpha$, there are only two different candidates for the images of these four embeddings: one real $\mathbb{Q}(\sqrt[4]{2})$ and one "imaginary" $\mathbb{Q}(i\sqrt[4]{2})$.

171. With $F := \mathbb{Q}(i)$ in the role of the ground field, $x^4 - 2 = (x-\alpha)(x+\alpha)(x-i\alpha)(x+i\alpha)$ factors completely in $F(\alpha)$ where $\alpha = \sqrt[4]{2}$. Note that no partial products of these linear factors belong to $F[x]$. Therefore $x^4 - 2$ is still irreducible over F. All the four embeddings of $F[x]/(x^4 - 2)$ into $\overline{\mathbb{Q}} \subset \mathbb{C}$ over $\mathbb{Q}(i)$ have the same range: once any of the four roots is adjoined to $\mathbb{Q}(i)$, the other 3 also lie in the field. Therefore the four different embeddings with the same image differ by a group consisting of four automorphisms (including the identity) of the field $F[x]/(x^4 - 2)$ over F. In fact it is rather obvious that they all are obtained by iterating the transformation $x \mapsto ix$ on $F[x]$, $x \mapsto ix \mapsto i^2x = -x \mapsto i^3x = -ix \mapsto i^4x = x$ i.e. form the cyclic group of order 4.

HW12

172. None of $x = 0, 1, -1 \in \mathbb{Z}_3$ is a root of $f := x^3 - x - 1$, and hence f is irreducible in $\mathbb{Z}_3[x]$. Therefore $F := \mathbb{Z}_3[x]/(f)$ is a field of degree 3 over $\mathbb{Z}_3$, i.e. consists of $3^3 = 27$ elements. The multiplicative group $F^\times$ is cyclic of order 26, whose elements' orders can be $1, 2, 13$, and 26. Let α denote the class of x in $\mathbb{Z}_3[x]/(f)$. Then $1, \alpha, \alpha^2$ form a basis of F over $\mathbb{Z}_3$. We have $\alpha^3 = \alpha + 1$, $\alpha^9 = (\alpha + 1)^3 = \alpha^3 + 1^3 = \alpha - 1$, and $\alpha^{13} = \alpha\alpha^3\alpha^9 = \alpha(\alpha + 1)(\alpha - 1) = \alpha^3 - \alpha = 1$. Since clearly -1 has order 2, we conclude that $-\alpha$ must have order 26, and is a generator of $F^\times$ (as well as any power $(-\alpha)^k$ with $0 < k < 26$ odd $\neq 13$).

184. Let's denote $\overline{x}$ by α (as in Exercise 172). We have: $\Phi(1) := 1^3 = 1$, $\Phi(\alpha) := \alpha^3 = \alpha + 1$, $\Phi(\alpha^2) := \alpha^6 = (\alpha + 1)^2 = \alpha^2 - \alpha + 1$. Therefore $M = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = I + N$, where N is upper-triangular. Thus $M^3 = (I + N)^3 = I^3 + N^3 = I$, since $N^3 = 0$ (as for any upper-triangular 3×3-matrix. Consider the polynomial $x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 :=$

$$(x - \alpha)(x - \Phi(\alpha))(x - \Phi^2(\alpha)) = (x - a)(x - \alpha - 1)(x - \alpha + 1).$$

(We use here that $\Phi^2(\alpha) = \alpha^9 = \alpha - 1$). We find:

$$\sigma_1 = \alpha + (\alpha + 1) + (\alpha - 1) = 3\alpha = 0,$$
$$\sigma_2 = \alpha(\alpha + 1) + \alpha(\alpha - 1) + (\alpha + 1)(\alpha - 1) = 3\alpha^2 - 1 = -1,$$
$$\sigma_3 = \alpha(\alpha + 1)(\alpha - 1) = \alpha^3 - \alpha = 1,$$

i.e. our polynomial is indeed $x^3 - x - 1 = f$.

188. Since the divisors of 6 are $1, 2, 3$ and 6, the general theory of finite fields shows that $\mathbb{F}_{2^6}$ contains $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$ (one copy of each),

whose intersection is $\mathbb{F}_{2^1} = \mathbb{Z}_2$ (since 2 and 3 are coprime). For every $\alpha \in \mathbb{F}_{2^6}$, the field $\mathbb{Z}_2(\alpha)$ (the smallest subfield containing α) must be one of these $\mathbb{F}_{2^n}$, $n = 1, 2, 3, 6$, and the minimal polynomial of α must have the respective degree n. There are 2 elements (0 and 1) in $\mathbb{F}_{2^1}$; their minimal polynomials (x and $x - 1$) have degree 1. There are $2 = 2^2 - 2^1$ more elements in $\mathbb{F}_{2^2}$ and $6 = 2^3 - 2^1$ more elements in $\mathbb{F}_{2^3}$; their minimal polynomials have degrees 2 and 3 respectively. Therefor there are $2^6 - 6 - 2 - 2 = 54$ remaining elements in $\mathbb{F}_{2^6}$, whose minimal polynomial must have degree 6. In fact each of these polynomials is a divisor of $x^{64} - x$ (since all $\alpha \in \mathbb{F}_{2^6}$ satisfy $\alpha^{64} = \alpha$). This polynomial has 64 simple roots, and hence all roots of the minimal polynomials discussed above are also simple. Besides, being irreducible over $\mathbb{Z}_2$, two different minimal polynomials must be coprime. Since each minimal polynomial of degree 6 is minimal for each of its 6 distinct roots, the number of such polynomials must be $54/6 = 9$.

193. The minimal polynomial over $\mathbb{Q}$ for α is $f = x^3 - 2$, and for β is $x^2 - 2$. The sufficient condition for $\theta = \sqrt[3]{2} + \sqrt{2}$ to serve as a primitive element is that it is not equal to any other sum $\alpha' + \beta'$ of roots of the respective polynomials. And indeed, the other root $-\sqrt{2}$ of g is also real, while the other two roots of $x^3 - 2$ are non-real. Thus $a + \beta = \alpha' + \beta'$ is impossible unless α' is real (hence $= \alpha$), in which case $b' = \beta$.

Now, $h(x) := g(\theta - x) = (\theta - x)^2 - 2 = x^2 - 2\theta x + (\theta^2 - 2)$ has $\alpha = \sqrt[3]{2}$ as a root, and must have a common factor with $f(x) = x^3 - 2$. Performing the Euclidean algorithm, we have:

$$f(x) - (x + 2\theta)h(x) = (3\theta^2 + 2)x + (-2\theta^3 + 4\theta - 2).$$

Since α is root of the L.H.S., we find $\sqrt[3]{2} = (2\theta^3 - 4\theta + 2)/(3\theta^2 + 2)$. This gives an expression of $\sqrt[3]{2}$ as an element of $\mathbb{Q}(\theta)$, and $\sqrt{2} = \theta - \sqrt[3]{2} = (\theta^3 + 6\theta - 2)/(3\theta^2 + 2)$ also lies in $\mathbb{Q}(\theta)$.

HW13

200. (a) The field E can be described as $\mathbb{Q}(\sqrt[4]{2}, i)$. It contains the subfield $\mathbb{Q}(\sqrt[4]{2} \cong \mathbb{Q}[x]/(x^4 - 2)$ of degree 4 over $\mathbb{Q}$ (e.g. because the polynomial $x^4 - 2$ is irreducible by Eisenstein's criterion with $p = 2$). Since $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ contains $\pm\sqrt[4]{2}$ but does not yet contain the other two roots $\pm i\sqrt[4]{2}$ of $x^4 - 2$, the splitting field must be obtained by adjoining $i = \sqrt{-1}$ (the ratios of the roots), and thus coincides with $\mathbb{Q}(\sqrt[4]{2}, i)$, which has therefore degree 8 over $\mathbb{Q}$. For a basis, putting $\alpha := \sqrt[4]{2} \in \mathbb{R}_{>0}$, one can take $1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3$.

(b) In fact it is clear *a priori* that the Galois group $G(E/\mathbb{Q})$, being a subgroup of order 8 in the group S_4, must be non-abelian, isomorphic to the dihedral group D_4. Indeed, since $|S_4| = 24$, a subgroup of order 8 must be one of the Sylow 2-subgroups, which are all conjugated (hence isomorphic), and in the rotation group of the cube (isomorphic to S_4), there are three such dihedral groups (formed by rotations of the cube interpreted as a square prism).

To describe the action of D_4 on the roots of $x^4 - 2$, consider the roots $\alpha, i\alpha, -\alpha, -i\alpha$ (we remind that $\alpha = \sqrt[4]{2}$) as the vertices of a square on the complex plane. The automorphism of E induced by mapping i to i and $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ induces the counter-clockwise rotation of this square through 90°. The complex conjugation $i \mapsto -i$ (and $\sqrt[4]{2} \mapsto \sqrt[4]{2}$) induces the reflection of the square about the real axis. The two transformations generate the dihedral (Galois) group.

(c) The groups D_4 has 3 subgroups of index 2 (all therefore normal): one isomorphic to $\mathbb{Z}_4$ and consisting of the rotations of the square, and 2 isomorphic to $\mathbb{Z}_2^2$, each consisting of two conjugated reflections of the square and the central symmetry (= rotation through 180°). The latter rotation also generates the normal subgroup $\mathbb{Z}_2$ (which happens to form the center of D_4), and each of the 4 reflections generate 4 non-normal subgroups isomorphic to $\mathbb{Z}_2$. The list of totally 10 subgroups is completed by the trivial group $\{e\}$.

The last subgroup corresponds of course to the whole field $E^{\{e\}} = E$. When the subgroup H is the normal $\mathbb{Z}_2$ (generated by the central symmetry) of the rectangle), that symmetry maps $i \mapsto i$, and $\alpha := \sqrt[4]{2} \mapsto -\alpha = -\sqrt[4]{2}$. In our basis $1, \alpha, \alpha^2, \alpha^3, i\alpha, i\alpha^2, i\alpha^3$, this symmetry acts by preserving $1, i, \alpha^2, i\alpha^2$ and changing the sign of $\alpha, \alpha^3, i\alpha, i\alpha^3$. The fixed points of it form the subspace spanned by $1, i, \alpha^2, i\alpha^2$, i.e. the subfield $\mathbb{Q}(\sqrt{2}, i)$ of degree 4 over $\mathbb{Q}$.

A similar analysis of conjugated reflections $\alpha, i\alpha \mapsto \alpha, -i\alpha$ and $\alpha, i\alpha \mapsto -\alpha, i\alpha$ shows that the fixed points form two conjugate subfields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(i\alpha)$ of degree 4 over $\mathbb{Q}$.

Analyzing fixed points of the other two conjugated reflections, which are $\alpha, i\alpha \mapsto i\alpha, \alpha$ and $\alpha, i\alpha \mapsto -i\alpha, -\alpha$ (both mapping $i \mapsto -i$), we will conclude that the corresponding fields are isomorphic to $\mathbb{Q}[x]/(x^4+2)$ and coincide with $\mathbb{Q}(\alpha(1-i)/\sqrt{2})$ and $\mathbb{Q}(\alpha(1+i)/\sqrt{2})$ respectively. (Namely, the 1st reflection interchanges α^3 with $-i\alpha^3$, and hence preserves their average $\alpha(1-i)/\sqrt{2}$, while the 2nd likewise preserves $\alpha(1+i)/\sqrt{2}$.)

The intersection of each of these 4 degree-4 subfields of E with the normal subfield $\mathbb{Q}(\sqrt{2}, i)$ yields the 2 degree-2 extensions of $\mathbb{Q}$ fixed by the 2 subgroups of D_4 isomorphic to $\mathbb{Z}_2^2$: $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$.

The subfield $\mathbb{Q}(i)$ corresponds to $\mathbb{Z}_4 \subset D_4$ (mapping $\alpha \mapsto i\alpha \mapsto -\alpha \mapsto -i\alpha \mapsto \alpha$, but fixing i), and of course the whole D_4 corresponds to $E^{D_4} = \mathbb{Q}$.

201. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the splitting field of the collection x^2-2, x^2-3, x^2-5 of three quadratic polynomials; so it is normal, is obtained by consecutively adjoining to $\mathbb{Q}$ the three square roots, has the basis $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{2\cdot 3}, \sqrt{2\cdot 5}, \sqrt{3\cdot 5}, \sqrt{2\cdot 3\cdot 5}$ over $\mathbb{Q}$, and Galois group isomorphic to $\mathbb{Z}_2^3$ and generated by independent changes of the signs of $(\sqrt{2}, \sqrt{3}, \sqrt{3}) \mapsto (\epsilon_1\sqrt{2}, \epsilon_2\sqrt{3}, \epsilon_3\sqrt{5}$, where $\epsilon_i = \pm 1$.

The group $\mathbb{Z}_2^3$ can be considered as a 3-dimensional vector space over $\mathbb{Z}_2$, and its subgroups as $\mathbb{Z}_2$-subspaces: there are 7 subspaces of dimension 1 (spanned by 7 non-zero vectors), and 7 subspaces of dimension 2 (given by 7 non-zero linear equations).

The 7 subfields, whose elements are fixed a corresponding non-trivial element $\epsilon = (\pm 1, \pm 1, \pm 1) \neq (1,1,1)$ of the Galois group are:

$$(-1,1,1) : \mathbb{Q}(\sqrt{3}, \sqrt{5}), \quad (1,-1,1) : \ \mathbb{Q}(\sqrt{2}, \sqrt{5}),$$
$$(1,1,-1) : \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad (-1,-1,1) : \ \mathbb{Q}(\sqrt{5}, \sqrt{6}),$$
$$(-1,1,-1) : \mathbb{Q}(\sqrt{3}, \sqrt{10}), \quad (1,-1,-1) : \ \mathbb{Q}(\sqrt{2}, \sqrt{15}),$$
$$(-1,-1,-1) : \mathbb{Q}(\sqrt{6}, \sqrt{10}) \ \text{ (note that } \sqrt{15} = \sqrt{6}\sqrt{10}/2).$$

Writing $\epsilon = ((-1)^a, (-1)^b, (-1)^c)$ with $a, b, c \equiv 0, 1 \mod 2$, we have 7 non-trivial linear equations of 2-dimensional subgroups, and the corresponding subfields of their fixed elements:

$$a \equiv 0 : \mathbb{Q}(\sqrt{2}), \quad b \equiv 0 : \ \mathbb{Q}(\sqrt{3}), \quad c \equiv 0 : \ \mathbb{Q}(\sqrt{5}),$$
$$a+b \equiv 0 : \mathbb{Q}(\sqrt{6}), \quad a+c \equiv 0 : \ \mathbb{Q}(\sqrt{10}), \quad b+c \equiv 0 : \ \mathbb{Q}(\sqrt{15}),$$
$$a+b+c \equiv 0 : \mathbb{Q}(\sqrt{30})$$

208. Over $\overline{\mathbb{Z}_p}$, the polynomial $x^n - 1$ factors into linear factors (whose roots, therefore, are all nth roots of unity in characteristic p).

Let $n = p^r m$ where m is not divisible by p. Then $x^n - 1 = (x^m - 1)^{p^r}$, i.e. all nth roots of unity in characteristic p are actually mth roots of unity (occurring in $x^n - 1$ with multiplicity p^r). Since p^r and m are coprime, $\varphi(n)$ is divisible by $\varphi(m)$, and hence $\mathbb{F}_{p^{\varphi(m)}} \subset \mathbb{F}_{p^{\varphi(n)}}$. By Euler's theorem, $p^{\varphi(m)} \equiv 1 \mod m$, and therefore the cyclic group $\mathbb{F}^\times_{p^{\varphi(m)}}$ of order $p^{\varphi(m)} - 1$ contains all m distinct mth roots of unity.

`Remark.` When $n = m$ is not divisible by p, the solution amounts to the last sentence.

214. Let $\zeta := e^{2\pi i/5}$. The Galois group $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{Z}_5^\times$ is generated by $\sigma : \zeta \mapsto \zeta^2$. So, the sequence $\{\sigma^k(\zeta)\}$ is $\zeta, \zeta^2, \zeta^{-1}, \zeta^{-2}$. The Gauss sums generating the quadratic extension intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ are $\eta_+ := \zeta + \zeta^{-1} = 2\cos 2\pi/5$ and $\eta_- := \zeta^2 + \zeta^{-2} = 2\cos 4\pi/5$. They are roots of $x^2 + x - 1$ since $\eta_+ + \eta_- = -1 = \eta_+\eta_- = \zeta^3 + \zeta^{-1} + \zeta^1 + \zeta^{-3}$. Thus, $2\cos 2\pi/5 = (\sqrt{5} - 1)/2$ is the famous golden ratio, and can be easily constructed by straightedge and compass.