Answers and hints to homework problems.

HW1

1.1(6) A subset of the set $\{1, \ldots, n\}$ set is specified by n independent binary choices: to include each of $1, 2, \ldots, n$ into the subset or not. Thus there are 2^n subsets.

1.1(11) Any symmetric and transitive binary relation of a set S can be described as follows: S is represented as the disjoint union of subsets S' and S'', such that elements of S'' are not in the relation to any element of S, and the binary relation on S' is an equivalence relation (i.e. symmetric, transitive, and reflexive). When S'' is non-empty, reflexivity does not hold ttue on the whole of S. Thus the error in the "proof" that "$2 + 3 \Rightarrow 1$" is the tacit assumption that every $a \in S$ is in the relation with at least one $b \in S$.

1.2(7) In defining a permutation σ on the set $\{1, \ldots, n\}$, there are n choices for $\sigma(1)$, $n-1$ choices of $\sigma(2)(\neq \sigma(1))$, $n-2$ choices of $\sigma(3)(\neq \sigma(1), \sigma(2))$, etc., i.e. totally $n \times (n-1) \times (n-2) \times \cdots \times 1 = n!$ choices.

1.3(7b) Using the Euclidean algorithm, we find $(6540, 1206) = 6$.

1.3(10a) If the set of those $n \geq m_0$ for which $P(n)$ is false is non-empty, then it has the minimal element $m > m_0$ (since $P(m_0)$ is true), and hence $P(m-1)$ is true, in conflict with the hypothesis that $P(m-1) \Rightarrow P(m)$ holds true for all $m > m_0$.

1.3(17) $[a][b] = [0]$ in $\mathbf{Z}_n$ is equivalent to $n|ab$. The fact that $n|ab$ implies $n|a$ or[1] $n|b$ is the definition of n being prime.

Cantor–Bernstein Theorem. Given injectiones $f : A \to B$ and $g : B \to A$, construct a bijection $h : A \to B$ as follows. If the sequence $a, g^{-1}(a), f^{-1}g^{-1}(a), \ldots$ does not terminate or terminates with an element from B, put $h(a) = g^{-1}(a)$. If it terminates with an element in A, then put $h(a) = f(a)$.

HW2

2.3(1c) Yes, this is a group ismorphic to $\mathbf{Z}_7$.

2.3(3) Multiplying $(ab)(ab) = a^2b^2$ by a^{-1} on the left and b^{-1} on the right, obtain: $ba = ab$ (for all $a, b \in G$), i.e. the group G is abelian.

2.3(7) In S_3, the three transpositions and the identity satisfy $x^2 = e$, and the two ciclic shifts and the identity satisfy $y^3 = e$.

2.3(11) The operation $x \mapsto x^{-1}$ pairs each element with its inverse, unless the element is its own inverse, i.e. satisfies $a^2 = e$. If the order of the group is even, there have to be even number of solutions to $a^2 = e$, and since one is $a = e$ there must exist another such a.

[1] The formulation *and* in the book is an error

2.3(25) (a) The matrix enties are taken from $\mathbf{Z}_3$ (whose elements can be added and multiplied). To have a non-zero 2×2 determinant the 1st column (a, c) can be any except $(0, 0)$ (which gives $3^3 - 1 = 8$ choices), while the secod column (b, d) must be non-proportional to (a, c) (which gives $3^2 - 3 = 6$ choices). Thus the order of the group is $8 \times 6 = 48$.
(b) Furthermore, dividing the 2nd column by the (non-zero, i.e. equal to $\pm 1 \in \mathbf{Z}_3$) value of the determinant, we obtain a matrix with the determinant $= 1$. Thus the order of the group of such matrices is $48/2 = 24$.

Compute the determinant of the $n \times n$-matrix with all entries on the diagonal equal to 2, right under and right above the diagonal -1, and 0 everywhere else.

Let Δ_n denote the determinant. Using the expancion with respect to the 1st row, and then the expansion of the 2nd determianant of size $n-1$ with respect to the 1st column, we obtain the following recursion: $\Delta_n = 2\Delta_{n-1} - \Delta_{n-2}$. It follows by induction on n that $\Delta_n = n + 1$.

HW3

2.5(3) If $G (\neq \{e\})$ has no non-trivial subgroups, then it must coincide with the cyclic group of any of its non-identity elements, and thus must be cyclic itself, and of prime order (since cyclic groups of infinite or composite order do have non-trivial subgroups).

2.5(5) The operation $x \mapsto x^{-1}$ of inversion on a group G transforms left H-cosets to right H-cosets, and in particular establishes a 1–1 correspondence between them.

2.5(15) The center Z of a group G (i.e. the set of those elemets which commute with all elements of the group) is the centralizer $C(H)$ (formed by those elemets of G which commute with all elemets from a subgroup H) of the whole group, i.e. $Z = C(G)$.

2.5(29) $\mathbf{Z}_8^\times$ has 4 elements $1, 3, 5, 7$ and is not cyclic since all of its elements satisfy $x^2 = 1$.

2.7(2) On a group G, the conjugation $x \mapsto gxg^{-1}$ by a given element $g \in G$ is an automorphism (called *interior*), because: $(gxg^{-1})(gyg^{-1}) = gxyg^{-1}$ for all $x, y \in G$.

Groups G and G'. The inversion operation $x \mapsto x^{-1}$ establishes an isomorphism of a group G with the group G' (defined as the same set G but equipped with the opposite product $a \cdot b := ba$) because $(ba)^{-1} = a^{-1}b^{-1}$.

HW4

2.6(1) If $\forall a, b,\ HaHb \subset Hab$, then $\forall a \in G, h \in H, \exists h' \in H$ such that $eahe = h'ae$, i.e. $aha^{-1} = h' \in H$.

2.6(2) If $[G:H]=2$, then one of the two cosets is H, and the other (no matter left or right) is its complement $G\backslash H$.

2.6(8) Take $G=GL_2(\mathbf{R})$, H the set of *integer* upper-triangular matrices with 1s on the diagonal, and a the diagonal matrix with the entries diagonal entries 2 and 1 in the 1st and 2nd rows respectively.

2.6(13) Every subgroup of a cyclic group T is invariant under every automorphism of T. Indeed, if $T\cong\mathbf{Z}$, then the only non-trivial automorphism of T is the inversion $t\mapsto t^{-1}$, which leaves each subgroup invariant. When $T\cong\mathbf{Z}_n$ is finite, then for each $m|n$ there is only one subgroup in $\mathbf{Z}_n$ of order n/m (namely, $m\mathbf{Z}_n$), and hence any automorphism of $\mathbf{Z}_n$ must leave this subgroup invariant. When T is a normal subgroup of G, then conjugation by any $a\in G$ preserves T and acts on it by an automorphism. Thus each subgroup of T is invariant under conjugations by any elements of G and is therefore normal in G.

2.7(5ab) Put $xyx^{-1}y^{-1}=:z$. Then $gzg^{-1}=(gzg^{-1}z^{-1})(xyx^{-1}y^{-1})$, i.e. congugation of a commutator $xyx{-}1y^{-1}$ by g is the product of two commutators. Therefore the subgroup G' generated by commutators is invariant under conjugations and hence normal. In G/G' we have: $[x][y][x]^{-1}[y]^{-1}=[xyx^{-1}y^{-1}]=G'=[e]$. Thus $[x][y]=[y][x]$, i.e. G/G' is abelian.

2.7(19) If $a=\det A, b=\det B$, then $\det ABA^{-1}B^{-1}=aba^{-1}b^{-1}=1$. Thus the commutator subgroup G' of $G=GL_2(\mathbf{R})$ lies in N. To show that $\det A=1$ implies that $A\in G'$, note that A can be written as the product (in a certain order) of a lower-triangular matrix with 1s on the diagonal, an upper-triangular matrix with 1s on the diagonal, a diagonal matrix, and possibly the matrix $\begin{bmatrix}0&-1\\1&0\end{bmatrix}$. (These factors correspond to elementary row operations which reduce a matrix to the identity.) An upper-(lower-) triangular matrices with 1s on the diagonal are commutators of upper-(lower-)triangular matrices with diagonal ones (like in 2.6(8)), which therefore lie in G'. Products of such matrices (one lower- and one upper-triangular) yield matrices with arbitrary values of the trace, and in particulr, matrices *similar* to diagonal matrices with arbitrary eigenvalues $\lambda\neq\lambda^{-1}$ — which therefore also lie in G' (because G' is normal). We have:

$$\begin{bmatrix}0&-1\\1&0\end{bmatrix}=\begin{bmatrix}1&-1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix}\begin{bmatrix}1&-1\\0&1\end{bmatrix}\in G'.$$

Finally, powers of this matrix yield $\pm I$ which are the only diaginal matrices with eigenvalues $\lambda=\lambda^{-1}$.

The 6th grade problem. It is required to find a positive integer x such that $2(10x+2) = x + 2 \cdot 10^n$, where n is the number of decimal digits in x. We have: $2(10^n - 2) = 19x$, i.e. we need to find n such that $10^n \equiv 2 \bmod 19$. Note that $20 \equiv 1 \bmod 19$, i.e. $2 \equiv 10^{-1} \bmod 19$. By the LFT, $10^{18} \equiv 1 \bmod 19$, and hence $10^{17} \equiv 10^{-1} \equiv 2 \bmod 19$. Thus $x = 2(10^{17} - 2)/19$ will do.

HW5

2.7(13) The center of a dihedral group $D_n, n \geq 3$, is trivial when n is odd and consists of $\pm I$ when n is even. Indeed, congugating a rotation by reflection we get a rotation in the opposite direction. The only way how it can coincide with the original one is if the rotation is through π i.e. is the central symmetry $-I$ (which indeed commutes with all linear transformations). Since $n \geq 3$, the group contains rotations other than $\pm I$ which do not commute with any reflection, and so the latter ones cannot lie in the center.

2.7(14) The commutator subgroup $D_n' \subset D_n$ must lie in the kernel of the determinant homomorphism, i.e. in the subgroup of rotations through the angles multiple to $2\pi/n$. Computing commutators of (a) two reflections, (b) a rotation and reflection (two rotations in D_n commute), we find them to be rotations through angles multiple of $4\pi/n$. For odd n they generate the whole cyclic group of rotations; for even n, they generate only the cyclic subgroup of index 2 in it.

2.8(7a) A subgroup invariant w.r.t. all automorphisms is invariant w.r.t. interior ones in particular, which are conjugations by elements of the groups. Thus such a subgroup is normal.

2.8(16) An integer a satisfies $a^n \equiv 1 \bmod (a^n - 1)$, and geberates the multiplicative cyclic subgroup $\{1, a, a^2, \dots, a^{n-1}\}$ of order n. By Langange's theorem, n divides the order $\phi(a^n - 1)$ of the multiplicative group $\mathbf{Z}_{a^n-1}^{\times}$.

2.10(22) The symmetry group D_n of a regular n-gon can be realized by permutations of its n. Taking a rotation through $2\pi/n$ and one of the reflections as generators of D_n, we can represent them by the permutations: $(1, 2, \dots, n-1, n)$ (one cycle of length n) and $(1, n)(2, n-1)(3, n-2)\dots$ ($[n/2]$ 2-cycles) respectively. Of course, Cayley's theorem provedes another repesentation of D_n — as a subgroup in S_{2n}.

A. The isomorphism between the rotation group of the cube and S_4 is obtained by associating to a rotation the permutation it induces on the set of 4 diagonals of the cube.

B. Since $\mathbf{Z}_n$ is generated by 1, a homomorphism $\Phi : \mathbf{Z}_n \to \mathbf{Z}_n$ is determined by $k := \Phi(1) \in \mathbf{Z}_n$. It is surjective (and hence bijective) only when $\Phi(1)$ is relatively prime to n. Let Ψ be another homomorphism, such that $\Psi(1) = l$. Then the composition $\Psi(\Phi(1)) = \Psi(k) = kl$. i.e. the operation in the group of automorphisms coincides with the multiplication operation in $\mathbf{Z}_n^\times$.

HW6

2.8.(5) If ϕ is an automorphism of a group G, and ψ_g is the interior automorphism definied as the conjugation $x \mapsto gxg^{-1}$ by an element $g \in G$, then $\phi\psi_g\phi^{-1}(x) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)x\phi(g)^{-1}$, i.e. $\phi\psi_g\phi^{-1}$ is the automorphism of conjugation by $\phi(g)$.

2.9(8) In a group G of $2p$ elements (p prime), a Sylow p-subgroup has order p (if $p \neq 2$) and is normal as any subgroup of index 2. If $p = 2$, then $o(G) = 4$, and G (whether cyclic or not) must have an element of order 2.

2.10(11) Conjigations of the transposition $(1, 2)$ by powers of the cyclic shift $(1, 2, \ldots, n)$ yield transpositions $(2, 3), (3, 4), \ldots, (n - 1, n)$ of any pair of consecutive indices, which obviously generate the whole group S_n. (Think of lining up a row of n people according to their heights by comparing neighbors and transposing them when necessary.)

2.10(13) If a normal subgroup of A_n contains a 3-cycle (say, $(1, 2, 3)$), then it contains all 3-cycles. Indeed, permuting the entries in the Yuoung tableaux $(1, 2, 3)(4)(5) \ldots (n)$, we can get any 3-cycle (a, b, c), and if the permutation happened to be odd, we can transpose a and c and thus get the inverse 3-cycle (c, b, a) as a conjugation of $(1, 2, 3)$ by an element of A_n. In either case, both (a, b, c) and (c, b, a) will lie in the subgroup, if one of them lies there. Now, any subgroup of A_n containing all 3-cycles coincides with A_n since the product of any pair of transpositions (commuting or not) can be written as a product of 3-cyces:

$$1234 \mapsto 3124 \mapsto 3412 \text{ is } (13)(24), \text{ and } 123 \mapsto 213 \mapsto 231 \text{ is } (123).$$

2.11(7) The order of a permutation is the Least Common Multiple (LCM) of the lengths of its cycles. In S_p (p prime), the order p of a permutation means that it has one cycle of length p. All such permutations form one conjugacy class containing $p!/p = (p-1)!$ permutations. Elements of S_p satisfying $x^p = e$ are these $(p - 1)!$ permutations plus 1 more: the identity.

Problem. *Show that the group of rotations of a dodecahedron is isomorphic to the alternating group A_5.*

Each of the 12 pentagonal faces of the dodecahedron has 5 diagonals, all of the same length. The key observation is that these 60 diagonals are edges of 5 cubes. (Each cube has 12 edges — one in each face of the dodecahedron.) The 5 cubes are permuted by the symmetry group of the dodecahedron. This defines a homomorphism $G \to S_5$ of the group G of rotations of the dodecahedron to the group of permutations. It is easy to see geometrically that rotations of order 5 (about centers of faces) 3 (about vertices), and 2 (midpoints of edges) generate permutations of the 5 cubes which are: a 5-cycle, a 3-cycle, and the product of two commuting 2-cycles respectively. (Think how the diagonals in a face, around a vertex, and next to an edge are permuted.) All such permutations are even and non-trivial. Thus the range of the homomorphism lies in A_5, the kernel is trivial, and since both groups G and A_5 are known to have the same order 60, the monomorphism must be bijective.

HW7

2.11(17) In a group G of order 15, the number of Sylow subgroups P of order 5 must be congruent to 1 modulo 5 but cannot exceed $3 = 15/5$ (since such subgroups form one orbit under conjugations, and the normalizer of P contains P). Thus there is only one subgroup, $P \cong \mathbf{Z}_5$, of order 5 which is therefore normal. Conjugations by G act on P by automorphisms, which defines the homomorphism: $G \to G/P \to Aut(P)$. Since $Aut(\mathbf{Z}_5) \cong \mathbf{Z}_5^\times$ has order 4, and G/P has order 3, we conclude that the homomorphism is trivial, i.e. P lies in the center of G. Let x be a generator of P, and $y \notin P$. If y has order 15, then it generates G which is therefore cyclic. If y has order 3, then, since y commutes with x, we have: $G \cong \mathbf{Z}_5 \times \mathbf{Z}_3 \cong \mathbf{Z}_{15}$.

2.12(5) Partition the set $\{1, \ldots, p^2\}$ into p subsets of order p:

$$\{1, \ldots, p\}, \ldots, \{(p-1)p + 1, \ldots, p^2\}.$$

Then the p permutations:

$$(1, \ldots, p), \ldots, ((p-1)p + 1, \ldots, p^2)$$

(each is a cycle of order p) generate a subgroup of S_{p^2} isomorphis to $\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ (p times). Together with the cyclic shift σ of those p subsets (i.e. the permutation $\sigma(1) = 1 + p,\ \sigma(2) = 2 + p,\ \ldots$) they generate a subgroup of order p^{p+1}. It is a Sylow p-subgroup of S_{p^2} since $(p^2)!$ contains the factor of p exactly $p^2/p + p^2/p^2 = p + 1$ times.

2.12(8) In a group G of order 231, the number of elements in the orbit of a Sylow subgroup $P \cong \mathbf{Z}_{11}$ under conjugations must divide $231/11 = 21$ and have remainder 1 modulo 11. Thus it is unique, and hence normal. Now, conjugations by G/P act trivially on P since the order $\phi(11) = 10$ of $Aut(P) \cong \mathbf{Z}_{11}^{\times}$ is relatively prime to $o(G/P) = 21$. Thus P is central.

2.12(20) The group $GL_n(\mathbf{Z}_p)$ of invertible $n \times n$-matrices with entries from $\mathbf{Z}_p$ (p a prime) has the order $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$. (Any non-zero column of n entries from $\mathbf{Z}_n$ as the 1st column, any column non-proportional to the 1st one as the 2nd column, any column which is not a linear combination of the 1st and 2nd column as the 3rd one, etc.) The maximal power of p which divides this product is $0+1+2+\cdots+(n-1)$. The subgroup of upper-triangular matrices with 1 on the diagonal and arbitrary entries from $\mathbf{Z}_p$ above the diagonal has the required order and is therefore a Sylow p-subgroup of $GL_n(\mathbf{Z}_p)$.

2.13(5) We did this in class. In a finite abelian group G of order $p_1^{n_1} \cdots p_k^{n_k}$ (p_i are distinct primes, $n_i > 0$), the Sylow p_i-subgroups G_i have orders $p_i^{n_i}$. Consider the map

$$G_1 \times \cdots \times G_k \to G : \quad (g_1, \ldots, g_k) \mapsto g_1 \cdots g_k.$$

It is a homomorphism (since G is abelian), and its kernel is trivial. Indeed, if $g_1 \cdots g_k = e$, then $g_1 = (g_2 \cdots g_k)^{-1}$ has the order which is a common factor of $p_1^{n_1}$ and $p_2^{n_2} \cdots p_k^{n_k}$. Thus $g_1 = g_2 \cdots g_k = e$, and by induction, $g_2 = \cdots = g_k = e$ as well. Therefore the homomorphis is injective, and since $o(G_1 \times \cdots \times G_k) = o(G)$, it is surjective as well.

Problem. *Prove that if p^k (p prime) divides the order of — a group G, then G has a subgroup of order p^k.*

This is obvious for cyclic groups. In general, passing to a Sylow p-subgroup, we may assume that $o(G) = p^n$, $n \geq k$. Use induction on n. If $n = 1$, then the trivial subgroups have orders p^0 and p^1. For arbitrary n, we want to find subgroups of G of orders p^{n-1} and apply the induction hypothesis. The group G has a non-trivial center Z. Take in Z any non-trivial cyclic subgroup, and a subgroup Z' of order p in it. Then G/Z' has the order p^{n-1}. Thus G/Z' contains a subgroup of order p^{n-2}, and its inverse image in G is a subgroup of order p^{n-1}.

HW8

2.13(4ab). Since the operation in $G \times G$ is component-wise, it is obvious that $G \to G \times G : g \mapsto (g, g)$ is a group homomorphism, Since its composition with the projection $G \times G \to G : (g_1, g_2) \mapsto g_1$ is the identity map $G \to G$, the image Δ of the first map is isomorphic to G. If Δ is normal, then $(e, x)(g, g)(e, x^{-1}) = (g, xgx^{-1} \in \Delta$ for all $x, g \in G$, i.e. $g = xgx^{-1}$, or equivalently: $gx = xg$.

2.13(7). When $(m, n) = 1$, and hence the $L.C.M.(m, n) = mn$, the homomorphism $\mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n : x \mapsto (x \bmod m, x \bmod n)$ has the kernel $mn\mathbf{Z}$, and hence the range containing mn elements. It is therefore surjective.

2.13(11). The group G is isomorphic to the direct product of cyclic groups whose orders are powers of primes. Since the factors are subgroups with pairwise trivial intersection, there can be only one factor, i.e. $G \cong \mathbf{Z}_{p^n}$ for some prime p and $n > 0$.

2.13(15). When $G = \mathbf{Z}_p \times \mathbf{Z}_p$ (p prime), $Aut(G) = GL_2(\mathbf{Z}_p)$, and hence G has $(p^2 - 1)(p^2 - p)$ automorphisms.

2.13(16). The center of the direct product of groups is the direct product of the factor's centers, because arrays $(x_1, ..., x_n)$ and $(y_1, ..., y_n)$ commute in the direct product if and only if they commute componentwise.

2.14(6). Let $G \cong \mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_k}}$, where p is prime. Let Δ be the Young diagram whose rows contain $n_1 \geq \cdots \geq n_k > 0$ cells. Suppose H is a subgroup in G, and Δ' is the corresponding Young diagram. We will prove by induction on the nuber of cells in Δ that Δ' is contained in Δ. This is obvious for the trivial group G (the base of induction). Now, consider the homomorphism $G \to G : x \mapsto x^p$. The kernel of it contains p^{n_1} elements, and its range is a subgroup $\tilde{G}$ whose diagram is obtained by discarding the 1st row of Δ. The same homomorphism restricted to H has the kernel containing p^{h_1} elements where $h_1 \leq n_1$, and the range $\tilde{H} \subset \tilde{G}$. We conclude that the number h_1 of cells in the 1st row of Δ' does not exceed n_1. Furthermore, applying the induction hypothesis to the groups $\tilde{H} \subset \tilde{G}$, we conclude that by discarding the 1st rows of Δ' and Δ we obtain two diagrams of which the former is contained in the latter. Thus the same is true about the original diagrams Δ' and Δ.

HW9

3.2(3). In an associative ring, $(a_0 + a_1)^n$ expands as the sum of 2^n monomials $a_{i_1} \cdots a_{i_n}$, where each $i_k = 0$ or 1. Generally speaking, this sum contains no similar terms.

3.2(7,11) $\mathbf{Z}_p[x]$ is an example of an infinite integral domain of finite characteristic p, and (along with $\mathbf{Z}$) also provides an example of integral domain that is not a field.

3.2(12). In a field, there are no divisors of zero; namely if $ab = 0$ but $a \neq 0$, then $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

3.2(14). To prove that the decimal representation of every fraction p/q is repeating, consider the process of long division of p by q, each step of which consists in finding the next decimal digit as the quotient of division by q of the remainder of the previous division. Since there are only q possible remainders (including 0), after no more than q steps some of the previous remainders will occur again, and the therefore the algorithm will enter the mode of cyclic repetition.

The King Arthur Problem. Let $f_0 : \mathbf{Z}_n \to \mathbf{R}$ be the function on the set of knights (which of course are elements of the cyclic group $\mathbf{Z}_n$) describing the initial (i.e. at $T = 0$) distribution of cereal. Let $g : \mathbf{Z}_n \to \mathbf{R}$ be the function equal to $1/2$ at 1 and -1, and equal to 0 everywhere else on $\mathbf{Z}_n$. Then the distribution of cereal at a moment $T > 0$ is given by the function $f_T = g^{*T} f_0 = (g * \cdots * g) * f_0$ (i.e. is the convolution by g applied T times to f_0). Since the Fourier transform $f \to \hat{f}$ on $\mathbf{C}[\mathbf{Z}_n]$ transfroms convolution into pointwise product of functions, we have: $\hat{f}_T = \hat{g}^T \hat{f}_0 = (\hat{g} \cdots \hat{g})\hat{f}_0$. Let us compute the value of $\hat{g}$ (which is a function of the group of characters of $\mathbf{Z}_n$) at the character $\phi_l : \mathbf{Z}_n \to U : k \mapsto e^{2\pi i k l/n}$ (here k, l are integers modulo n). We have:[2]

$$\hat{g}(l) = \sum_{k=0}^{n-1} g(k)\phi_l(-k) = \frac{e^{-2\pi i l/n}}{2} + \frac{e^{2\pi i l/n}}{2} = \cos(2\pi l/n).$$

When $l \neq 0$ or $n/2$, the values of $\cos(2\pi l/n)$ are smaller than 1 in the absolute values, and therefore their powers $(\cos 2\pi l/n)^T$ tend to 0 as $T \to \infty$. When the number n of knights is odd (and thus $n/2$ is not an integer), the only exception is $\hat{g}(0) = \cos 0 = 1$. We have in this case:

$$\hat{f}_\infty := \lim_{T\to\infty} \hat{f}_T = \lim_{T\to\infty} \hat{g}(l)^T \hat{f}_0(l) = \left\{ \begin{array}{c} \hat{f}_0(0) \text{ if } l = 0 \\ 0 \text{ if } l \neq 0 \end{array} \right. .$$

The inverse Fourier transform then yields the distribution f_∞ of sereal in the limit $T \to \infty$:

$$f_\infty(k) = \frac{1}{n}\sum_{l=0}^{n-1} \hat{f}_\infty(l)\phi_l(k) = \frac{1}{n}\hat{f}_0(0)\phi_0(k).$$

[2] In other words: eigenvalues of the operator of convolution by g are $\cos(2\pi l/n)$, $l = 1, \ldots, n$.

Since $\phi_0(k) = 1$ for all k, and $\hat{f_0}(0) = \sum f_0(k)$, we conclude that in the case of odd n, the amount of cereal is redistributed as $T \to \infty$ evenly between the knights. A similar analysis for even n shows that as T becomes large, the amount of cereal for knights at even (respectively odd) seats becomes the same, and equal at even moments of T to the their average initial amount, and at the odd moments of T becomes equal to the everage initial amount of knights at the odd (respectively even) seats.

HW10

3.4(3). A field F has only the trivial ideals $\{0\}$ and F, and therefore each homomorphism from F is either injective (when the kernel is $\{0\}$, or zero (when the kernel is F).[3]

3.4(12). To prove that the ring M of all $n \times n$ matrices has no nontrivial two-sided ideals J, let us prove that together with any nonzero matrix A, the ideal J contains each of matrices E_{ij} all of whose entries are 0 except the ijth entry equal to 1. Let v be a vector such that $Av \neq 0$. Introduce the linear transfromation B in $\mathbf{R}^n$ which sends all unit coordinate vectors e_k to 0 except e_j mapped to v. Take any linear transformation C that maps $w = Av$ to the unit coordinate vector e_i. Then $CAB = E_{ij}$. Thus, if $A \in J$, then every $E_{ij} \in J$, and therefore every sum of scalar multiples of the matrices E_{ij} is in J, and thus $J = M$.

3.4(20). If a ring homomorphism $\phi : R \to R'$ is surjective, then for every $a' \in R'$ there is $a \in R$ such that $\phi(a) = a'$. Then $\phi(1)a' = \phi(1a) = \phi(a) = a' = \phi(a) = \phi(a1) = a'\phi(1)$. Thus $\phi(1)$ is the unit element in R'.

3.6(5bdef). We proved this in class for $S = R - 0$, and the proof is the same word-for-word for an arbitrary multiplicative system S.

3.6(6). If $(m, n) = 1$, then we may assume there exist $k, l > 0$ such that $km - ln = 1$. Then $a^{km} = b^{km}$, and hence $ac = bc$ where $c = a^{ln} = b^{ln}$. In an integral domain, this implies: $a = b$.

HW11

Ch. 3 (4). If a commutative ring R with the unit element is finite, then for every prime ideal I, the quotient integral domain R/I is also finite, and is therefore a field. hence the ideal I is maximal.

Ch 3 (8). In a commutative ring R, if A is an ideal, and $x^n, y^m \in A$, then $(x+y)^l = \sum \binom{l}{k} x^k y^{l-k} \in A$ if $l \geq m+n$. Thus the radical $N(A)$ is an additive subgroup. Also, for every $z \in R$ we have: $(zx)^n = z^n x^n \in$

[3] The formulation in the book is erroneous: an injection (e.g. $\mathbf{R} \subset \mathbf{C}$ does not have to be an "isomorphism."

A, and so $N(A)$ is an ideal. Furthermore, if $a^s \in N(A)$, then there exists n such that $A \ni (a^s)^n = a^{ns}$, i.e. $a \in N(A)$.

A. Let $f(x, y)$ be a non-constant polynomial with complex coefficients. We can write it as $f = x^n g_0(y) + \cdots + g_n(y)$ where g_i are polynomials in y, and assume (possibly after switching the roles of x and y) that $g_0 \neq 0$. Since g_0 has at most finitely many roots, we can pick infinitely many complex values $y = y_1, y_2, \ldots$ such that $g_0(y_i) \neq 0$, and then for each y_i, find a complex root x_i of the degree $n > 0$ polynomial $f(x, y_i)$. Then (x_i, y_i), $i = 1, 2, \ldots$ form infinitely many solutions to the equation $f(x, y) = 0$.

B. Hilbert's Nullstellensatz applied to $1 \in \mathbf{C}[x_1, \ldots, x_n]$ and an ideal $I = (f_1, ..., f_k)$, shows that if the system $f_1 = \cdots = f_k = 0$ has no complex solutions, then for some $n > 0$, $I \ni 1^n = 1$, and hence I is trivial. This property fails over $\mathbf{R}$, as the example of the ideal $(x^2+1) \subset \mathbf{R}[x]$ shows: the equation $x^2 + 1 = 0$ has no real solutions, but 1 is not divisible by $x^2 + 1$.

C. `Answer.` Maximal ideals in $\mathbf{C}[x, y]$ are $(x-a, y-b)$, where $a, b \in \mathbf{C}$ in $\mathbf{R}[x]$ are $(x - a)$ and $(x^2 - 2ax + a^2 + b^2)$ where $a \in RR, b \in \mathbf{R}^\times$; for an ideal $I \subset \mathbf{R}[x, y]$, if the algebraic set X_I has no points in $\mathbf{C}^2$, then $1 \in I$, and hence $I = \mathbf{R}[x, y]$. Thus, if the ideal I is maximal, it must coincide with its radical, and define a non-empty algebraic set $X_I \subset \mathbf{C}^2$. If X_I consist of one real point (a, b), or a pair of complex conjugate points $(a, b), (\bar{a}, \bar{b})$, then the corresponding ideal $I = (x - a, y - b)$ in the first case, and in the second consists of all polynomilas with real coefficients vanishing at these two complex conjugate points. The generators of the latter ideal can be taken as: $(x-a)(x-\bar{a})$, $(y-b)(y-\bar{b})$, $(x - a)(y - \bar{b}) + (x - \bar{a})(y - b)$. When X_I contains more than one of: a real point, a pair of complex conjugate points, the ideal cannot be maximal, since it is contained in the kernels of at least two different evaluation homomorphisms.

HW12

3.7(7). The condition $a|x$ and $b|x$ means $(x) \subset (a) \cap (b)$. In a PID, the ideal $(a) \cap (b) = (c)$ for a suitable element c. Since $(x) \subset (c)$ means $c|x$, we conclude that $c = [a, b]$ (least common multiple of a and b).

3.7(8). If $a = \prod p_i^{k_i}$, $b = \prod p_i^{l_i}$ are prime factorizations of a and b, then it follows from the unique factorization theorem, that $(a, b) = \prod p_i^{\min(k_i, l_i)}$, $[a, b] = \prod p_i^{\max(k_i, l_i)}$, and hence $[a, b] = ab/(a, b)$.

3.8(3b). Using the Euclidean algorithm in $\mathbf{Z}[i]$, we find:

$$18 - i = (11 + 7i) + (7 - 8i), \ 11 + 7i = i(7 - 8i) + 3,$$

$$7 - 8i = (2 - 3i)3 + (1 + i), \ 3 = (1 + i)(1 - i) + 1,$$

and hence $(18-i, 11+7i)=1$.

3.8(4). Since a prime $p=4n+3$ cannot be factored in $\mathbf{Z}[i]$, we find that $F:=\mathbf{Z}[i]/(p)$ is a field. Then the polynomial x^2+1 factors as $(x-i)(x+i)$ in $F[x]$, and cannot have factors of the form $x-a$, $a\in\mathbf{Z}/p\mathbf{Z}\subset F$. Thus x^2+1 has no roots in $\mathbf{Z}/p\mathbf{Z}$.

3.8(6). Let $p_1,...,p_k$ be some primes of the form $4n-1$. Then $p_1\cdots p_k+2$ (when k is even) or $p_1\cdots p_k+4$ (when k is odd) is congruent to -1 modulo 4 and thus must be divisible by at least one prime of the form $4n-1$, but is not divisible by any of $p_1,...,p_k$. Thus no finite set of promes of the form $4n-1$ exhausts all of them.

A. $5=(2+i)(2-i)$, $13=(3+2i)(3-2i)$, $17=(4+i)(4-i)$, and thus there are four ways of writing $5\cdot 13\cdot 17$ as $(a+bi)(a-bi)$ which are essentially different (i.e. are not obtained from each other by changing (a,b) to $(\pm a,\pm b)$ or $(\pm b,\pm a)$), namely:

$$a+bi=(2+i)(3+2i)(4+i),\ a+bi=(2-i)(3+2i)(4+i),$$

$$a+bi=(2+i)(3-2i)(4+i),\ (2+i)(3+2i)(4-i).$$

Multiplying out, we find respectively:

$$a+bi=9+32i,\ a+bi=31+12i,\ a+bi=33+4i,\ a+bi=23+24i.$$

Thus

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

B. Let $p_1\cdots p_k=a^2+b^2=(a+bi)(a-bi)$. Then, since $(a+bi)$ must have a non-integer prime factor, at least one of p_i must also have such a factor in $\mathbf{Z}[i]$. Such a p_i cannot be of the form $4n-1$.

HW13

3.9(3). If $f,g\in F[x]$ are relatively prime, then $1=af+bg$ for some $a,b\in F[x]$, and this remains true in $K[x]$ hence for any field $K\supset F$.

3.9(7). If $f\in F[x]$ is irreducible of degree n, then $E:=F[x]/(f)$ is a field extension of F of dimension n as a vector space over F, and when F is finite and consists of of q elements, then $K\cong F^n$ consists of q^n elements.

3.10(2). When p is prime, x^n-p is irreducible over $\mathbf{Q}$ by the Eisenstein criterion.

3.10(5). If $a=m/n$ is rational, and $x-a$ divides a monic integer polynomial, then n divided the top coefficient 1 of this polynomial, and hence $n=\pm 1$, and $a=\pm m$ is an integer.

Suppl. Prob. in Ch 3 (18). If F is a finite field, then there is a smallest positive integer p such that $0=1+\cdots+1$ (p times), and since $(1+\cdots+1)(1+\cdots+1)=1+\cdots+1$ (m times, n times, and mn times), the number p must be prime (otherwise F would have divisors of 0). Moreover, the cyclic subgroup of $(F, +)$ generated by 1 is in fact the subfield $\mathbf{Z}/p\mathbf{Z}$. Then F is a vector space over $\mathbf{Z}/p\mathbf{Z}$ of a certain finite dimension p, and hence consists of $q = p^n$ elements. The order of the multiplicative group $F^\times$ is $q - 1$, and hence $a^{q-1} = 1$ for every $a \neq 0$. It follows, that $a^q = a$, which remains true even for $a = 0$.

Besides, if the abelian group $F^\times$ were not cyclic, it would follow (from the classification of finite abelian groups) that there exists a proper divisor n of $q - 1$, such that $a^n = 1$ for all $a \in F^\times$. This would yield a degree n polynomial, $x^n - 1$, having $q - 1 > n$ roots, which is impossible. Thus $F^\times$ is cyclic.

HW14

5.1(3a). If V is a vector space over K with a basis $v_1, ..., v_n$, and the degree m field extension $K \supset F$ has a basis $u_1, ..., u_m \in K$ as a vector space over F, then $\{u_j v_i\}$ form a basis of V as a vector space over F.

5.1(4). Let $a = \sqrt{2} + \sqrt{6}$. Then $a^2 = 5 + 2\sqrt{6}$, and $a^4 = 49 + 20\sqrt{6}$. Therefore $a^4 - 10a^2 + 1 = 0$. The polynomial $f := x^4 - 10x^2 + 1$ has four roots $\pm\sqrt{2} \pm \sqrt{3}$, none of which is rational, and no *two* of which have rational sum *and* product. This shows that f has no factors in $\mathbf{Q}[x]$ of degree 1 or 2, and thus f is irreducible over $\mathbf{Q}$. Thus the degree of $\mathbf{Q}(a)$ over $\mathbf{Q}$ is 4, while the degree of $\mathbf{Q}(\sqrt{6})$ over $\mathbf{Q}$ is 2.

5.4(7c). The degree 3 polynomial $f := x^3 + x^2 - 2x - 1$ is irreducible over $\mathbf{Q}$ since it has no rational roots. (Indeed, only $m/n = \pm 1$ could qualify, but the coefficient sum of f is odd.)

5.4(8). Take $a = e^{2\pi i/7}$, and put $b = a + a^{-1} = 2\cos 2\pi/7$. Then $b^2 = a^2 + a^{-2} + 2$, $b^3 = a^3 + 3a + 3a^{-1} + a^{-3}$. Thus

$$b^3 + b^2 - 2b - 1 = 1 + a + a^2 + a^3 + a^{-3} + a^{-2} + a^{-1} = 0$$

as the total sum of the 7th roots of unity.

5.4(13). A circle cannot be divided by straightegde and compass into 9 congruent arcs, because each arc would measure 40°, and bisecting it, one would construct the angle of 20°, which is impossible.

Problem. If $(m, n) = 1$, then $1 = am + bn$ for some integers a and b. Therefore

$$\frac{2\pi}{mn} = a\frac{2\pi}{n} + b\frac{2\pi}{m},$$

i.e. the central angle $2\pi/mn$ can be constructed from $2\pi/n$ and $2\pi/m$ by adding (subtracting) $|a|$ copies of the former and $|b|$ copies of the latter.