KTH Teknikvetenskap

SF2729 Groups and Rings
Suggested solutions to the final exam
Wednesday, August 17, 2011

PART I - GROUPS

(1) (a) A *latin square* of size $n \times n$ is an $n \times n$-array of symbols where each symbol occurs exactly once in each row and in each column. Show that the multiplication table of a finite group has to be a latin square. **(2)**

(b) Let G be the set of invertible 2×2-matrices with coefficients in $\mathbb{Z}_6$. Show that G is a group under matrix multiplication. **(2)**

(c) Lagrange's theorem states that the order of a subgroup H of a finite group G divides the order of G. Prove this theorem. **(2)**

SOLUTION

a). Because every element is invertible, we can solve any equation $a * x = b$ uniquely by multiplication by a^{-1} to the left. We get $a^{-1} * (a * x) = a^{-1} * b$, which by the associativity is equivalent to $(a^{-1} * a) * x = a^{-1} * b$. Since $a^{-1} * a = e$, and $e * x = x$, we get $x = a^{-1} * b$. This means that the symbol b occurs exactly once in the row given by a. In the same way, we apply multiplication on the right to $x * a = b$ to conclude that every symbol b occurs exactly once in the column corresponding to a.

b). Matrix multiplication is associative over any ring. The identity matrix, I_2, is a unit and all invertible matrices have a two-sided inverse. The only thing that remains to check is that the product of two invertible matrices, A and B, is invertible. This is true since

$$(B^{-1}A^{-1})(AB) = B^{-1}I_2B = B^{-1}B = I_2$$

and similarly $(AB)(B^{-1}A^{-1}) = I_2$.

c). We first show that the left cosets of H form a partition of G. This can be done by introducing the equivalence relation

$$a \sim_L b \Leftrightarrow a^{-1}b \in H$$

We check that this is indeed an equivalence relation.

$i)$ (*reflexivity*) $a^{-1}a = e \in H$, for all $a \in G$.

$ii)$ (*symmetry*) $(a^{-1}b)^{-1} = b^{-1}a$ and hence $a^{-1}b \in H \Leftrightarrow b^{-1}a \in H$ since H is a subgroup.

$iii)$ (*transitivity*) If $a^{-1}b \in H$ and $b^{-1}c \in H$, we get $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

Now, we check that $a \sim_L b$ if and only if they are in the same coset. In fact, $a^{-1}b \in H \Leftrightarrow b \in aH$.

Since the equivalence classes give a partition of the set, we get that the left cosets give a partition of the set G into disjoint subsets. (Of course this also holds for the right cosets.)

Once we know that the cosets, which all have size $|H|$, form a partition of G, we get that $|G|$ has to be a multiple of $|H|$.

---

(2) Let G be the group of invertible 2×2-matrices with entries in $\mathbb{Z}_6$ from problem 1(b) and let G act on $\mathbb{Z}_6 \times \mathbb{Z}_6$ seen as column vectors by matrix multiplication. Let $x = (1, 0) \in \mathbb{Z}_6 \times \mathbb{Z}_6$.

(a) Determine the stabilizer G_x. [1] **(2)**

(b) Determine the orbit Gx. **(2)**

(c) Use the results of part (a) and (b) to determine the order of G. **(2)**

SOLUTION

a). The matrices that stabilize x satisfy

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

where the arithmetics is done in $\mathbb{Z}_6$. This means that $a = 1$, $c = 0$, while b and d are arbitrary. Now we are only interested in the matrices in G, so they have to be invertible. This means that d has to be invertible and b can still be arbitrary. In $\mathbb{Z}_6$ only ± 1 are invertible. Thus we have the twelve elements

$$\begin{bmatrix} 1 & b \\ 0 & \pm 1 \end{bmatrix}$$

b). The orbit is given by all elements that can be written as

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}$$

where the 2×2-matrix is invertible. By the usual formula from linear algebra, we know that if a matrix is invertible, its inverse can be written as

$$\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Thus the matrix is invertible if and only if the determinant is invertible. In this setting, this means that the determinant is ± 1. We look for the possible a and c such that we can find b and d with $ad - bc = \pm 1$. This is impossible if a and c have a common factor which is not invertible. There are $3 \cdot 3 = 9$ cases where 2 is a common factor and $2 \cdot 2 = 4$ cases where 3 is a common factor. One of these is common, $(0, 0)$.

When neither 2 nor 3 is a common factor, the equation $ax - cy = 1$ can be solved over $\mathbb{Z}_6$. Thus the orbit consists of all $36 - 12 = 24$ pairs (a, c), where a and c don't have 2 or 3 as a common factor.

c). We have in general that for a finite group $|G| = |Gx| \cdot |G_x|$. In our case we have computed the order of the stabilizer to be twelve and the size of the orbit to be twenty-four. Thus we get

$$|G| = |Gx| \cdot |G_x| = 12 \cdot 24 = 288.$$

---

[1] The stabilizer is also called the *isotropy subgroup*.

(3) Let $\Phi\colon G \longrightarrow H$ be a surjective group homomorphism and $K \leq H$ a normal subgroup.
(a) Show that the inverse image $\Phi^{-1}(K)$ is a normal subgroup of G. **(2)**
(b) Show that $G/\Phi^{-1}(K)$ is isomorphic to H/K. **(2)**
(c) Assume that K equals the commutator subgroup $[H, H]$. Show that $\Phi^{-1}(K)$ contains $[G, G]$. Does equality hold? **(2)**

SOLUTION

a). If a is in $\Phi^{-1}(K)$ and b is any element of G we get that

$$\Phi(bab^{-1}) = \Phi(b)\Phi(a)\Phi(b)^{-1}$$

which is in K since $\Phi(a) \in K$ and K is normal in H. Thus bab^{-1} is in $\Phi^{-1}(K)$ which shows that $\Phi^{-1}(K)$ is normal in G.

b). We have the natural homomorphism $\Psi : H \longrightarrow H/K$ and when we compose it with Φ, we get $\Psi\circ\Phi : G \longrightarrow H/K$. This is surjective since both Φ and Ψ are surjective. Thus we have by the first isomorphism theorem that H/K is isomorphic to $G/\ker(\Psi \circ \Phi)$. It remains to show that $\ker(\Psi \circ \Phi) = \Phi^{-1}(K)$. Indeed, we have that

$$\ker(\Psi \circ \Phi) = \{a \in G | \Psi(\Phi(a)) = eK \in H/K\} = \{a \in G | \Phi(a) \in K\} = \Phi^{-1}(K).$$

c). The commutator subgroup is generated by all the commutators, $aba^{-1}b^{-1}$, where $a, b \in H$. It is sufficient to show that the image of any commutator in G is in K. This is true since

$$\Phi(aba^{-1}b^{-1}) = \Phi(a)\Phi(b)\Phi(a)^{-1}\Phi(b)^{-1}$$

which is a commutator in H. Thus any commutator lies in $\Phi^{-1}([H, H]) = \Phi^{-1}(K)$.

Another way is to use part (b) and see that H/K is abelian and since $G/\Phi^{-1}(K)$ is abelian, $\Phi^{-1}(K)$ has to contain the commutator subgroup, $[G, G]$.

Equality can of course hold, for example when Φ is an isomorphism. However, it is not an equality in general. If G and H are abelian, their commutator subgroups are trivial, but a surjective homomorphism $\Phi : G \longrightarrow H$ does not have to be injective.

PART II - RINGS

(1) (a) Let F be a finite field. Assume that -1 is not a square in F. Prove that 2 or -2 is a square in F. **(2)**
(b) Prove that $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$. **(2)**
(c) Let p be a prime number and let $\mathbb{F}_p$ be a finite field with p elements. Prove that $X^4 + 1$ is reducible in $\mathbb{F}_p[X]$. (Hint: use part (a) when -1 is not a square in $\mathbb{F}_p$.) **(2)**

SOLUTION

a). If $\mathrm{char}(F) = 2$, then $-1 = 1$ is a square in F. So $\mathrm{char}(F) = p$, an odd prime, and F has an odd number of elements (p^n for some $n \geq 1$). So $F^* = F\backslash\{0\}$ has an even number of elements. We know that F^* is cyclic (any finite subgroup of the invertible elements of a domain is cyclic). If x generates F^*, then the squares in F^* form the subgroup generated by x^2. It is of index 2 in F^* and the unique nontrivial coset consists of the nonzero nonsquares. So the product of two nonzero nonsquares is a nonzero square. So if 2 is a nonsquare, then -2 is a square, since -1 is a nonsquare.

b). $X^4 + 1$ clearly has no roots in $\mathbb{Z}$ (or $\mathbb{R}$). The only possible factorization is as a product of two polynomials of degree 2. One way to argue is by looking at the complex roots $\pm\frac{1}{2}\sqrt{2}\pm\frac{1}{2}i\sqrt{2}$ ($= e^{2\pi ik/8}$, k odd). We get that the factors in $\mathbb{R}[X]$ are $X^2\mp\sqrt{2}X+1$, which aren't in $\mathbb{Z}[X]$.

Another way: if $X^2 + aX + b$ is one factor in $\mathbb{Z}[X]$, one sees that the other factor must be $X^2 - aX + b$ (by looking at the coefficients of X^3 and X). Then $b^2 = 1$, so $b = \pm1$, and $a^2 = 2b = \pm2$, which doesn't have solutions in $\mathbb{Z}$.

Finally, a separate argument: $(X + 1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$ is irreducible by the Eisenstein criterion for $p = 2$, so $X^4 + 1$ is irreducible as well.

c). If -1 is a square f^2 in $\mathbb{F}_p$, then $X^4+1 = X^4-(-1) = (X^2)^2-f^2 = (X^2+f)(X^2-f)$ in $\mathbb{F}_p[X]$. If -1 is not a square, then $X^4 + 1$ certainly has no roots in $\mathbb{F}_p$. But 2 or -2 is a square in $\mathbb{F}_p$. Following the second argument in (b), we find $a \in \mathbb{F}_p$ with $a^2 = 2$ or $a^2 = -2$. Taking $b = +1$ resp. -1, we find a factorization in $\mathbb{F}_p[X]$. (Alternatively, $X^4 + 1 = X^4 \pm 2X^2 + 1 - (\pm2X^2) = (X^2 \pm 1)^2 - (\pm2X^2)$ is a difference of two squares, hence factorable, if ±2 is a square.)

(2) (a) Prove that $3+2i$ is a prime element of $\mathbb{Z}[i]$. **(2)**
(b) Prove that $F=\mathbb{Z}[i]/\mathbb{Z}[i](3+2i)$ is a field. How many elements does F have? **(2)**
(c) Find a generator of the multiplicative group of F. **(2)**

SOLUTION

a). Recall that $\mathbb{Z}[i]$ has a Euclidean norm N with $N(a+bi)=a^2+b^2$, which is multiplicative. The elements with norm 1 are the units ± 1, $\pm i$. The ring $\mathbb{Z}[i]$ is a UFD (even a PID). The norm of $3+2i$ equals 13, which is a prime number. It follows directly that $3+2i$ is irreducible, hence prime (since the ring is a UFD).

b). Nonzero prime ideals in a PID are in fact maximal, so $\mathbb{Z}[i]/\mathbb{Z}[i](3+2i)$ is a field F. In F, $13=(3+2i)(3-2i)=0$, so $\mathrm{char}(F)=13$. It is clear that F has at most 26 elements ($a+bi$ with $0\le a\le 12$ and $0\le b\le 1$), so in fact F has 13 elements (the only possible power of 13). (We also find this using $7(3+2i)=8+i=0$.)

c). The 13 elements of F can be thought of as a (modulo $(3+2i)$), with $0\le a\le 12$. We try the powers of 2:

$$2,\ 4,\ 8,\ 16=3,\ 2^5=6,\ 2^6=12.$$

So the order of 2 is 12 and 2 generates F^*. Other generators are $2^5=6$, $2^7=11$, and $2^{11}=7$.

(3) (a) Prove that the ring $\mathbb{R}[X]/(X^3 - X^2 + 2X - 2)$ is isomorphic to $\mathbb{R} \times \mathbb{C}$. **(2)**

(b) Let p be a prime number. Let R be the subring of $\mathbb{Q}$ consisting of the numbers a/b with $a, b \in \mathbb{Z}$ and b not divisible by p. Let I be a nonzero ideal of R. Prove that $I = (p^n)$ for some $n \geq 0$. Conclude that R has a unique maximal ideal. **(4)**

SOLUTION

a). In a commutative ring R with 1, two ideals I and J are called relatively prime when $I + J = R$ (i.e., $1 = i + j$ for some $i \in I$ and $j \in J$). One always has the inclusion $IJ \subseteq I \cap J$; equality holds when I and J are relatively prime, since for $a \in I \cap J$

$$a = a \cdot 1 = a(i + j) = ai + aj \in IJ.$$

The natural ring homomorphism

$$R/(I \cap J) \to R/I \times R/J, \qquad a + (I \cap J) \mapsto (a + I, a + J)$$

is injective. When I and J are relatively prime, it is surjective:

$$aj + bi + (I \cap J) \mapsto (a + I, b + J)$$

if $1 = i + j$. So, for two relatively prime ideals I and J, we obtain isomorphisms

$$R/IJ \cong R/(I \cap J) \cong R/I \times R/J;$$

this is commonly referred to as the Chinese Remainder Theorem.

Now $X^3 - X^2 + 2X - 2 = (X - 1)(X^2 + 2)$ and the two irreducible factors are relatively prime in $\mathbb{R}[X]$. By the above, we obtain an isomorphism

$$\mathbb{R}[X]/(X^3 - X^2 + 2X - 2) \cong \mathbb{R}[X]/(X - 1) \times \mathbb{R}[X]/(X^2 + 2).$$

But $\mathbb{R}[X]/(X-1) \cong \mathbb{R}$ via $X+(X-1) \mapsto 1$ and $\mathbb{R}[X]/(X^2+2) \cong \mathbb{C}$ via $X+(X^2+2) \mapsto i\sqrt{2}$.

b). We note that R is indeed a subring; the sum and product of two rational numbers whose denominators are not divisible by p are rational numbers whose denominators are not divisible by p. The invertible elements are the rational numbers for which the numerator is not divisible by p either. Hence $(a/b) = (p^n)$ if (b is not divisible by p and) a is exactly n times divisible by p (i.e., $a = a'p^n$ for an integer a' not divisible by p). If I is a nonzero ideal, let m be the minimum of the nonnegative integers n thus obtained from the nonzero elements of I. (The minimum exists.) Then $I = (p^m)$. For $m = 0$, the ideal (p^m) equals R; but the ideal (p) is maximal, and it clearly is the unique maximal ideal.
