MATH 113: ABSTRACT ALGEBRA (AUTUMN 2007)
SOLUTIONS TO FINAL EXAMINATION

1. Let $Q(X) = X^5 - 3 \in \mathbb{Z}[X]$. **Show** that the ideal $(Q) \subseteq \mathbb{Z}[X]$ is prime but is not maximal.

Proof: We give a direct proof.

Note that by the Eisenstein criterion, Q is irreducible over $\mathbb{Q}$. Hence, the ideal generated by Q in $\mathbb{Q}[X]$ (let us call it J) is maximal and therefore prime. If f and g were elements of $\mathbb{Z}[X]$ with $fg \in (Q)$, then $fg \in J$. So either $f \in J$ or $g \in J$. Without loss of generality, $f \in J$. That is, there is some $h \in \mathbb{Q}[X]$ with $hQ = f$. We may write $h = \frac{1}{n}H$ where $n \in \mathbb{Z}_+$ is a positive integer and $H \in \mathbb{Z}[X]$ is an integral polynomial at least one of whose coëfficients is equal to ± 1. We wish to show that $n = 1$. So assume that $n > 1$. Multiplying both sides by n we have $HQ = nf$. Write $H = \sum h_j X^j$. Let i be the largest integer for which h_i is a unit in $\mathbb{Z}_n$. We compute that the coëfficient of X^{2+i} on the left hand side is $a_i - 2a_{2+j}$ which is not zero in $\mathbb{Z}_n$ as a_i is a unit but a_{2+j} is not. However, on the right, every coëfficient is divisible by n. This a contradiction. Therefore, $f \in (Q)$ and we have shown that (Q) is prime.

Consider the map $\pi : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$ given by reducing the coëfficients modulo two. The polynomial $X^5 - 3 \in \mathbb{Z}_2[X]$ is not a unit. Hence, $I := (X^2 = 3) \subsetneq \mathbb{Z}_2[X]$ is a proper ideal. Let $J := \pi^{-1}I$. Then J is a proper ideal of $\mathbb{Z}[X]$ which properly contains I (as $X^5 - 3 \in J$, $(X^5 - 3) \subseteq J$, but $2 \in J \smallsetminus (X^5 - 2)$ as no constant is a multiple of a nonconstant polynomial).

2. Let $S := \mathbb{R} \smallsetminus \{-1\}$ be the set of all real numbers other than minus one. Define $*$ on S by $a * b := a + b + ab$. **Prove** or **disprove**: $(S, *)$ is a group.

Proof:

- closure: If a and b are real numbers, then of course $a*b = a+b+ab$ is a real number. Suppose now that a and b belong to S but $a * b \notin S$. That is, $-1 = a * b = a+b+ab$. Adding one to both sides, we have $0 = 1+a+b+ab = (1+a)(1+b)$ which implies, as $\mathbb{R}$ is an integral domain, $a = -1$ or $b = -1$ contrary to out hypothesis.
- identity: Set $e := 0$. Then $e * b = 0 + b + 0b = b = b + 0 + 0b = b * e$.
- inverse: For $a \in S$, let $a^{-1} := \frac{-a}{1+a}$. As $a \neq -1$, it makes sense to divide by $1+a$. We compute $a * \frac{-a}{1+a} = a + \frac{-a}{1+a} + a\frac{-a}{1+a} = a + \frac{-a-a^2}{1+a} = a + \frac{-a(1+a)}{1+a} = a - a = 0$.
- associativity: For a, b and c in S we have $(a*b)*c = (a*b)+c+(a*b)c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc = a+(b+c+bc)+a(b+c+bc) = a + (b*c) + a(b*c) = a*(b*c)$

3. Let α, β and γ be three distinct complex numbers satisfying $X^3 + 6X + 1 = 0$. **Compute** $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}]$.

Date: 15 December 2007.

By the rational root criterion, $X^3 + 6X + 1$ is irreducible over $\mathbb{Q}$. Computing derivatives, we see that this polynomial defines an increasing function on $\mathbb{R}$ so that there is only one real root. Without loss of generality, call that real root α. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, but because $\beta \notin \mathbb{R} \subseteq \mathbb{Q}(\alpha)$, we have $[\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] > 1$. As α is a root of $X^3 + 6X + 1$, the polynomial $X - \alpha$ divides $X^3 + 6X + 1$ giving a quotient $Q(X) = X^2 + \alpha X + (6 - \alpha^2) \in \mathbb{Q}(\alpha)[X]$ which is satisfied by β. Therefore, $[Q(\alpha)(\beta) : \mathbb{Q}(\alpha)] = 2$. Finally, as β is a root of Q, the polynomial $X - \beta$ divides $X^2 + \alpha X + (6 - \alpha^2)$ with γ being a root of the quotient, $X + (\alpha - \beta)$. That is, $\gamma = \beta - \alpha$. Therefore, $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}(\alpha, \beta)][\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 1 \times 2 \times 3 = 6$

4. **Prove** or **disprove**: If p is a prime number and $a \in \mathbb{Z}_p$ is any element of the field of p elements, then the polynomial $X^p - a \in \mathbb{Z}_p[X]$ is *reducible*.

Proof: Every nonzero element of $\mathbb{Z}_p$ is a unit. Hence, the unit group has size $p - 1$ so that for any $b \in \mathbb{Z}_p \smallsetminus \{0\}$ we have $b^{p-1} = 1$. Multiplying both sides by b, we have $a^p = a$. Of course, $0^p = 0$ also. Thus, every element a of $\mathbb{Z}_p$ satisfies $a^p = a$. So, a is a zero of the polynomial $X^p - a$ implying that $X - a$ divides this polynomial. As $p > 1$, this means that $X^p - a$ is reducible.

5. **Compute** $11^{7,890,207}$ in $\mathbb{Z}_{504}$

We factor $504 = 8 \times 9 \times 7$. Hence, $\mathbb{Z}_{504} \cong \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_7$ and $\mathbb{Z}_{504}^\times \cong \mathbb{Z}_8^\times \times \mathbb{Z}_9^\times \times \mathbb{Z}_7^\times \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_6) \times (\mathbb{Z}_6)$. Therefore, the exponent of $\mathbb{Z}_{504}^\times$ is six. We compute that $7890207 \equiv 3 \pmod 6$. Thus, $11^{7890207} = 11^3 = 1331 = 323$ in $\mathbb{Z}_{504}$.

6. **Express** the factor group $(\mathbb{Z}_{20} \times \mathbb{Z}_{12})/\langle(6, 6)\rangle$ as a product of cyclic groups.

The order of 6 in $\mathbb{Z}_{20}$ is ten while in $\mathbb{Z}_{12}$ it is two. Hence, $\#\langle(6, 6)\rangle = 10$ so that the factor group is an abelian group of order twenty-four. Thus, it is isomorphic to the Cartesian product of $\mathbb{Z}_3$ with an abelian group of order eight. As the maximal 2-part of an element of $\mathbb{Z}_{20} \times \mathbb{Z}_{12}$ is four, the group of order eight must be either $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The element $(1, 0) + \langle(6, 6)\rangle$ has order four as the only element of $\langle(6, 6)\rangle$ of the form $(2, n)$ is $(2, 6)$. Therefore, the two-part of the quotient is $\mathbb{Z}_2 \times \mathbb{Z}_4$. That is, the factor group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$.

7. Let G be a group. Recall that the *center* of G is the normal subgroup $Z(G) := \{x \in G : (\forall g \in G) gx = xg\}$. **Prove** or **disprove**: If $G/Z(G)$ is cyclic, then G is abelian.

Proof: Let $g \in G$ so that $gZ(G)$ generates $G/Z(G)$. Let a and b be two elements of G. Then we may write $a = g^i x$ and $b = g^j y$ for some x and y in $Z(G)$ and integers i and j. Then $ab = g^i x g^j y =^{\text{because } x \in Z(G)} g^i g^j xy =^{\text{because powers of } g \text{ commute}} g^j g^i xy =^{\text{because } y \in Z(G)} g^j y g^i x = ba$. Thus, G is abelian.

8. **Prove** or **disprove**: If $f(x) \in \mathbb{Z}_4[x]$ is a unit, then f is a constant polynomial.

Disproof: Consider $f(x) = 2x + 1$. Then $f^2 = (4x^2 + 4x + 1) = 1$. Thus, $f = f^{-1}$.

9. Let E be an extension field of the field F. Let $\alpha \in E$ be algebraic of odd degree over F. **Show** that α^2 is algebraic of odd degree over F and that $F(\alpha) = F(\alpha^2)$.

Proof: As $F(\alpha)$ is a field, the element $\alpha^2 = \alpha \times \alpha \in F(\alpha)$ so that $F(\alpha^2) \subseteq F(\alpha)$. As α satisfies the polynomial $X^2 - \alpha^2 \in F(\alpha^2)[X]$, we have $[F(\alpha) : F(\alpha^2)] \leq 2$. We wish to show that this degree must be one. We have $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ and the number on the left is odd. Hence, each of $[F(\alpha) : F(\alpha^2)]$ and $[F(\alpha^2) : F]$ must be odd and finite. As $[F(\alpha) : F(\alpha^2)] \leq 2$, this forces $F(\alpha) = F(\alpha^2)$.

10. Let G be a group. Suppose that $N \trianglelefteq G$ is a normal subgroup having the property that for all a and b in G, the element $aba^{-1}b^{-1}$ belongs to N. **Prove** that G/N is abelian.

Proof: Let g and h be two elements of G/N. Represent them as $g = aN$ and $h = bN$ for some a and b from G. By the hypothesis on N applied to b^{-1} and a^{-1}, we know that $b^{-1}a^{-1}ba \in N$. Thus, $gh = (aN)(bN) = abN = abb^{-1}a^{-1}baN = baN = (bN)(aN) = hg$. As g and h were arbitrary elements of G/N, we have shown that G/N is abelian.